

Netzwerk- und Sprachmanagement

EINE INTEGRIERTE LÖSUNG FÜR FEHLER- UND PERFORMANCE-MANAGEMENT

- Überblick über Veränderungen in konvergenten Netzwerken und Managementanforderungen
- Best Practices für die Implementation der CA-Lösung für Netzwerk- und Sprachmanagement

RECHTLICHER HINWEIS

Copyright © 2007 CA. Alle Rechte vorbehalten. Alle Marken, Produktnamen, Dienstleistungsmarken oder Logos, auf die hier verwiesen wird, sind Eigentum der entsprechenden Rechtsinhaber. Diese Dokumentation dient nur zu Informationszwecken. CA stellt diese Dokumentation, soweit es das anwendbare Recht zulässt, so wie sie vorliegt ohne jede Gewährleistung zur Verfügung; dazu gehören, ohne sich jedoch darauf zu beschränken, stillschweigende Gewährleistungen der Marktgängigkeit, der Eignung für einen bestimmten Zweck und der Nichtverletzung. In keinem Fall haftet CA für Verluste oder unmittelbare oder mittelbare Schäden, die aus der Verwendung dieser Dokumentation entstehen; dazu gehören, ohne sich jedoch darauf zu beschränken, entgangene Gewinne, Investitionsverlust, Betriebsunterbrechung, Verlust ideeller Unternehmenswerte oder Datenverlust, selbst wenn CA über diesen Verlust oder Schaden informiert wurde. Diese Dokumentation darf ohne vorherige schriftliche Genehmigung von CA weder vollständig noch auszugsweise kopiert, übertragen, vervielfältigt, veröffentlicht, geändert oder dupliziert werden. Die Informationen in dieser Dokumentation sind geistiges Eigentum von CA und durch das Urheberrecht der Vereinigten Staaten von Amerika sowie internationale Verträge geschützt.

DANKSAGUNGEN

CA dankt den folgenden Personen für ihren Beitrag bei der Erstellung dieses CA Green Book:

Hauptautoren

Don LeClair
Sue Andersen
Jason Bryk
Roger Craig
Bill Donoghue
Justin Gagnon
Brian Gollaher
Andrew Haigh
Kathleen Hickey
Mark Hounslow
John Kane
Michael Marks
John Murdough
Barbara O'Toole
Pete Oliveira
Jason Warfield
Dianne Weiss

Die Hauptautoren und CA möchten sich bei den folgenden Beteiligten bedanken:

Ajei Gopal
Tricia Bancroft
Lynn Beck
Gregory Buonaiuto
Curtis Lehman
Peter Clairmont
Dan Lewis
Anders Magnusson
Alexandre Moscoso
Joe Pennachio
David Soares
Peter Skotny
Cheryl Stauffer
Tom Wilson

CA-PRODUKTFERENZEN

- CA Netzwerk- und Sprachmanagement
- eHealth®
- eHealth® for Voice
- SPECTRUM®
- eHealth® for Voice Policy Manager
- eHealth® E2E Console
- eHealth® Live Health
- eHealth® Traffic Accountant
- eHealth® Universal Workflow Integration Modules
- eHealth® Universal Data Integration Modules
- eHealth® Universal Wireless Integration Modules
- SPECTRUM® Infinity
- SPECTRUM® Integrity
- SPECTRUM® Xsight
- SPECTRUM® OneClick
- SPECTRUM® Service Manager
- SPECTRUM® Report Manager
- SPECTRUM® Alarm Notification Manager
- SPECTRUM® ATM Circuit Manager
- SPECTRUM® Configuration Manager
- SPECTRUM® Secure Domain Manager
- SPECTRUM® Frame Relay Manager
- SPECTRUM® Microsoft Operations Manager Connector
- SPECTRUM® Multicast Manager
- SPECTRUM® OSS Integrations
- SPECTRUM® QoS Manager
- SPECTRUM® Remedy ARS Gateway
- SPECTRUM® SNMPv3 Support
- SPECTRUM® VPN Manager
- SPECTRUM® Watch Editor
- SPECTRUM® Service Performance Manager
- SPECTRUM® Assurance Server Xsight
- SPECTRUM® Assurance Server Integrity
- SPECTRUM® Assurance Server Infinity

Inhaltsverzeichnis

Kapitel 1: Einführung	9
Allgemeine Informationen zu diesem Buch	9
Kurzfassung	10
Wachsende Anforderungen an das Netzwerk- und Sprachmanagement	10
Die CA-Lösung für Netzwerk- und Sprachmanagement	11
Kapitel 2: Herausforderungen beim Netzwerk- und Sprachmanagement	13
Entwicklung von der reinen Netzwerkdienstleistung zur Serviceimplementation	13
Auswirkungen auf die Netzwerkteams	14
Änderung der Anforderungen an die Netzwerkmanagement-Software	14
Kapitel 3: Die CA-Lösung für Netzwerk- und Sprachmanagement	17
EITM: Die Unternehmensvision von CA	17
Enterprise Systems Management	18
Mehrwert der CA-Lösung für Netzwerk- und Sprachmanagement	19
Ein Schlüsselbestandteil der EITM-Vision von CA	21
Netzwerk- und Sprachmanagement für die wichtigsten vertikalen Märkte	21
Serviceanbieter im Bereich Telekommunikation	21
Regierungen	22
Unternehmen	22
Die Komponenten der Lösung	23
eHealth	23
Die eHealth-Komponenten	24
Die Vorteile von eHealth	24
SPECTRUM	25
Die SPECTRUM-Komponenten	25
Die Vorteile von SPECTRUM	26
Integration von eHealth and SPECTRUM	26
eHealth for Voice	27
Die Vorteile von eHealth for Voice	27
Serviceangebote von CA Technology Services für Netzwerk- und Sprachmanagement	28
Bewertung der Situation – Erkennen der Lücken	29
CA-Reifemodelle	30
Entwurf – Entwicklung der geeigneten Lösung	30
Implementierung – Die Basis für den Erfolg der Lösung	31
Optimierung – Den Zeitpunkt für Änderungen erkennen	31
Warum Sie die Verfügbarkeit Ihrer Services CA Technology Services anvertrauen sollten ...	31
Wie die wichtigsten Leistungsmerkmale in der Lösung realisiert sind	32
Effektives Service-Level-Management	32
Proaktive Servicesicherung	33
Schnelle Lösung von Problemen	34
Vorausschauende Kapazitätsplanung	35
Kapitel 4: Implementierungsarchitektur für das Netzwerk- und Sprachmanagement	37
Komponenten der Netzwerkleistung	37
E2E Console	38
Live Health	38
Integrationsmodule	38
Distributed eHealth	39
Remote Poller	39
Report Center	40
Traffic Accountant	40

Komponenten des Netzwerkfehler-Managements	41
Assurance Server	41
OneClick	42
Watch Editor	43
Alarm Notification Manager	44
Frame Relay Manager	44
ATM Circuit Manager	45
Multicast Manager	46
QOS Manager	46
VPN Manager	47
SNMPv3	47
Secure Domain Manager	48
Configuration Manager	48
Report Manager	49
Service Performance Manager	49
Service Manager	50
Komponenten des Sprachmanagements	51
eHealth for Voice	51
eHealth for Voice Policy Manager	52
Implementierungsarchitekturen	52
Implementation für kleine und mittelständische Unternehmen	53
Implementation für große Serviceanbieter	53
Dimensionierung sowie Hardware- und Softwareanforderungen für Netzwerkleistungen	55
Dimensionierung sowie Hardware- und Softwareanforderungen für Network Fault Management	56
eHealth for Voice – Hardware- und Softwareanforderungen für Einzelplatzrechner und Datenbankserver	57
Kapitel 5: Einrichtung und Konfiguration der integrierten Lösung	59
Installation der CA-Lösungssoftware für Netzwerk- und Sprachmanagement	59
Installationsvoraussetzungen	59
Installationsschritte	60
Installation von SPECTRUM	60
Installation von SPECTRUM OneClick und Report Manager	61
Installation von eHealth	61
Installation von eHealth for Voice	62
Konfiguration der integrierten Lösung	63
Best Practices	63
Identifizierung von Ressourcen und deren Discovery (Erkennung) als Global Selections mit Hilfe von SPECTRUM	64
Importieren von Global Selections in eHealth	65
Strukturierung von Ressourcen durch Erstellung von eHealth-Gruppen	67
Planung der eHealth-Discovery von Global Selections	68
Netzwerk- und Sprachüberwachung	69
Einrichtung von Live Health	69
Weiterleitung von Live Health-Traps an SPECTRUM	72
Anpassung und Einplanung von Health-Berichten zur Weiterleitung von Traps	73
Konfiguration von eHealth for Voice zum Senden von Alerts an SPECTRUM	75
Konfiguration von SPECTRUM zur Erkennung des eHealth-Servers	76
Konfiguration von SPECTRUM zur Anzeige von eHealth-Alarmen	77
Systemwartung	78
Archive für Systemsicherungen	78
Best Practices für die Wiederherstellung von Daten	78
Kapitel 6: Sammeln der Systeminformationen von Agenten	79
Implementation und Administration von Systemagenten	79
Best Practices	79
Unterstützte Agenten	80
Voraussetzungen	81
Hinzufügen von Systemagenten in SPECTRUM	81
Unicenter NSM-Agenten	87
Hinzufügen von Systemagenten in eHealth	88

Erstellung von Performance-Berichten für Systemagenten	88
Übersichtsberichte	88
MyHealth-Berichte für Systeme	90
Health-Berichte für Systeme	90
Verwendung von Live Trend	90
Ausführung von Trend-Berichten für Systeme	92
Top-N-Berichte	94
Konditionale Kapazitätstrend-Berichte für Systeme	94
Kapitel 7: Service-Level-Management	95
Interviewverfahren	96
Interviewfragen	96
Allgemeine Fragen	96
Analyse- und Zuordnungsverfahren	98
Gliederung der Informationen zu Ressourcen	98
Darstellung der wechselseitigen Beziehungen zwischen Ressourcen	98
Segmentierung der Informationen und Zuordnung zu Servicemodellen	98
Beispiel für die Zuordnung von Unternehmensservices zu Servicemodellen	99
Erstellung von Servicemodellen und Beziehungen	101
Die wichtigsten Konzepte	101
Erstellung von Servicemodellen	102
Beispiel 1: Service für den Zugriff auf Kundenkonten	102
Beispiel 2: Erweiterung des Services zur Überwachung kritischer Prozesse	110
Implementierung von Beispiel 2 in SPECTRUM	112
Beispiel 3: Erweiterung des Services zur Einbindung eines Antwortzeitelements	116
Erstellung von SLAs	119
Die wichtigsten Konzepte	119
Erstellung von SLAs und Gewährleistungen	121
Beispiel 4: Ein SLA für den 'Service für den Zugriff auf Kundenkonten'	122
Implementierung des SLA für A to Z Account Access in SPECTRUM	129
Erstellung von Service- und SLA-Berichten	131
Ausführung von kundennahen Berichten in SPECTRUM Service Manager	131
Serviceverfügbarkeit nach: Name, Kunde, Eigentümer	132
Variable Health-Ebene für Serviceverfügbarkeit	134
Zusammenfassung der Services nach: Name, Kunde, Eigentümer	135
Variable Health-Ebene für Zusammenfassung der Services	135
SLA-Details nach Kunden	136
SLA-Bestand nach Kunden	137
SPECTRUM Service Manager: Interne Berichte	137
Zustand von Services nach Servicename	137
Inventar von Services	139
Die Top-N-Services mit der schlechtesten Performance	140
Die Top-N-Services mit der schlechtesten Performance einschließlich der möglichen Ausfallarten	141
Ausfälle bei den Top-N-Services mit der schlechtesten Performance	141
Ressourcen der Top-N-Services mit der schlechtesten Performance nach Gesamtausfallzeit	142
Aktueller und letzter SLA-Status nach Kunde	143
SLA-Zusammenfassung nach: Name, Kunde, Status	143
SLA-Zusammenfassung: Warnung oder Verletzung	144
SLA-Details nach: SLA-Name, Zeitbereich, n letzte Perioden	145
SLA-Details mit Ressourcenausfällen	148
Kundenspezifische SLA-Zusammenfassung	149
Kapitel 8: Proaktive Servicesicherung	151
Identifizierung potenzieller Probleme	151
Konfiguration von Live Health zur Beobachtung wachsender Probleme	152
Konfiguration von Health-Berichten zum Senden von Traps bei wachsenden Problemen ...	153
Senden von Sprach-Alerts an SPECTRUM	153
Reaktion auf Alarmaktionen in SPECTRUM	153

Kapitel 9: Vorausschauende Kapazitätsplanung	155
Identifizierung von nicht ausgelasteten Ressourcen	156
Lokalisierung von nicht ausgelasteten Ressourcen	156
Bestätigung der unzureichenden Auslastung	158
Vorgehensweise bei unzureichender Auslastung von Ressourcen	159
Anzeigen des ROI	160
Aktualisierung der Konfiguration	161
Identifizierung der überlasteten Ressourcen	161
Suche nach überlasteten Ressourcen	161
Bestätigung der überlasteten Ressourcen	162
Vorgehensweise bei Überlastung von Ressourcen	165
Planung zukünftiger Kapazitätsänderungen	166
Identifizierung potenzieller Kapazitätsänderungen	166
Analyse von Kapazitätstrends	168
Visualisierung von Kapazitätsänderungen	171
Vorgehensweise bei Kapazitätsänderungen	172
Planung von Sprachkapazitäten	173
Analyse von Sprachkapazitäten	173
Analyse von GoS	174
Vorgehensweise bei unzureichender Auslastung von Ressourcen	176
Anzeigen des ROI	176
Bestätigung und Vorgehensweise bei Überlastung von Ressourcen	177
Analyse des Festplattenspeichers für Voice Messaging	177
Lösung von Festplattenspeicherproblemen	178
Kapitel 10: Schnelle Problemlösung	179
Verfahren zur Problemlösung	179
Komplexe Probleme und leistungsfähige Lösungen	180
Vorhersage von Problemen und Vermeidung	181
Auswirkungen auf das Unternehmen	181
Ereigniskorrelation und RCA – Ein dreiteiliger Ansatz	182
RCA	182
Verfahren zur induktiven Modellierung	183
Das Ereignis-Management-System	184
Korrelation der Bedingungen	186
Fehlerszenarien	188
Kommunikationsausfälle und deren Auswirkungen	188
Isolierung von Kommunikationsausfällen auf Basis der SPECTRUM-Informationen	189
Das Ereignis-Management-System	194
Anwendung der Bedingungskorrelation auf die Korrelation von Services	201
Effektiver Einsatz der integrierten Lösung	203
Index	205

Kapitel 1: Einführung

Allgemeine Informationen zu diesem Buch

Das CA Green Book für Netzwerk- und Sprachmanagement beschreibt, wie Sie die Leistung und Verfügbarkeit von konvergenten Netzwerken steuern können. Diese CA-Lösung ermöglicht das proaktive Management von Sprach- und Datendiensten und stellt gleichzeitig sicher, dass ausreichend Bandbreite und Systemkapazitäten zur Verfügung stehen. Darüber hinaus werden verschiedene unternehmensgesteuerte Service-Level unterstützt. Die Lösung ermöglicht außerdem ein integriertes Netzwerkfehler- und Performance-Management und unterstützt damit das Netzwerk in seiner Aufgabe als Plattform zur Bereitstellung von Services.

Die in diesem Buch enthaltenen Informationen richten sich an Netzwerkbetreiber, Ingenieure und andere technische Mitarbeiter, die mit dem Management von Sprach- und Datennetzwerken betraut sind. Die Implementationsbeispiele in diesem Buch stellen die Sichtweise eines kleinen Unternehmens und eines großen Serviceanbieters dar. Diese Informationen können auch für viele andere Netzwerkimplementationen hilfreich sein, sind jedoch ggf. nicht auf alle spezifischen Anforderungen zugeschnitten.

Das CA Green Book vermittelt ein Verständnis von den Möglichkeiten, die Ihnen heutzutage bei der Verwaltung konvergenter Netzwerke zur Verfügung stehen. Die einführenden Abschnitte bieten einen strategischen Überblick über die Trends, die im Bereich der konvergenten Netzwerke zu beobachten sind. In den darauffolgenden Abschnitten werden Best Practices zur Implementation und Verwendung der CA-Lösung für Netzwerk- und Sprachmanagement vorgestellt, die Sie bei der Verwaltung Ihres konvergenten Netzwerks unterstützen werden.

Die in diesem Buch enthaltenen Informationen beziehen sich ausschließlich auf das Netzwerk- und Sprachmanagement. Das Buch ist Bestandteil einer Reihe von CA Green Books, in denen die wesentlichen Funktionen einzelner CA-Lösungen erläutert und Best Practices vorgestellt werden, mit denen Sie die Lösungen verwalten und ausreichend sichern können. In anderen CA Green Books wird ein breites Spektrum an Themen aus dem Bereich IT-Management behandelt, wie z. B. das Management von Systemen und Datenbanken sowie die Automatisierung der anfallenden Arbeitslast.

Das CA Green Book für Netzwerk- und Sprachmanagement richtet sich an IT-Vorstände sowie Netzwerkmanagement- und Technikerteams. Das Buch ist wie folgt gegliedert:

- **Kapitel 1-3** bieten IT-Vorständen und Netzwerkverwaltern einen Überblick über die Herausforderungen bei der Verwaltung konvergenter Netzwerke und verdeutlichen den Stellenwert der CA-Lösung für Netzwerk- und Sprachmanagement.
- **Kapitel 4-10** zeigen Netzwerkverwaltern und anderen technischen Mitarbeitern Beispiele für die Implementation der Produkte auf, die in der CA-Lösung für Netzwerk- und Sprachmanagement zum Einsatz kommen. Sie enthalten Best Practices zur Planung, Implementation und Konfiguration dieser Lösung, um den Zeitraum zu verkürzen, bis sich die für die Optimierung des Netzwerks erbrachten Investitionen auszahlen.

In diesem CA Green Book werden folgende Themen behandelt:

- Technische Beschreibung der Komponenten, die die Grundlage für die empfohlene Lösung bilden
- Best Practices zur Einrichtung und Konfiguration der in der Lösung bereitgestellten Komponenten
- Definition und Verwaltung des Netzwerk-Service-Level-Managements
- Best Practices für proaktive Servicesicherung und schnelle Lösung von Problemen
- Durchführung von Kapazitätsplanungen und Verwaltung von Sprach- und Datennetzwerken

Kurzfassung

Wachsende Anforderungen an das Netzwerk- und Sprachmanagement

Bisher war die gesamte EDV-Infrastruktur vom jeweiligen Netzwerk abhängig. In jüngster Zeit hat sich der Einsatz von Netzwerken allerdings drastisch geändert, da mit der Bündelung von Daten, Sprache, geschäftskritischen Anwendungen und Videoinhalten alle Informationen über ein gemeinsames Netzwerk übertragen werden. Netzwerkfehler und Leistungsprobleme wirken sich daher unmittelbar auf die Produktivität, die Kosten und den Ertrag von Unternehmen aus.

Aus diesem Grund hat das Interesse und Bewusstsein für Netzwerkfehler und Leistungsprobleme eine größere Zielgruppe von unternehmensorientierten Anwendern aus nicht technischen Bereichen erreicht, die Informationen in Echtzeit benötigen. Zur Unterstützung konvergenter Daten- und Sprachnetzwerke müssen sich Netzwerkteams schnell neue Techniken aneignen und die Aufgabenbereiche innerhalb des Netzwerkmanagements erweitern.

Unter diesen Gegebenheiten müssen Netzwerkmanagement-Lösungen kritische Informations- und Verwaltungsfunktionen bieten, die Techniker und andere Anwender im Unternehmen gleichermaßen ansprechen. Zum Umfang dieser Lösungen sollten neben den traditionellen Funktionen des Fehler- und Performance-Managements auch konfigurierbare Warnungen, Dashboards sowie weitere analytische Funktionen gehören, die für alle Benutzer zugänglich sind.

Heutige Lösungen zum Netzwerk- und Sprachmanagement müssen folgende Merkmale unterstützen:

- **Heterogene Netzwerke** Sie müssen verschiedene Datenübertragungstechniken, z. B. Internet Protocol (IP), Asynchronous Transfer Mode (ATM), Frame Relay (FR) und Breitbandübertragung, unterstützen sowie Sprachinfrastrukturen, die aus herkömmlichen TDM-Infrastrukturen (Time-Division Multiplexing), speziellen IPT-Infrastrukturen (IP Telephony) und hybriden Infrastrukturen zusammengesetzt sind.
- **Skalierung** Sie müssen flächendeckende Netzwerke unterstützen, die über Länder und Kontinente hinweg einsetzbar sind und von zentralen oder regionalen Netzwerkmanagementteams verwaltet werden.
- **Integration** Sie müssen mit nur einer Lösung sowohl Daten- und Sprachinfrastrukturen als auch kritische Systeme verwalten können.

- **Rollenbasierte Serviceinformationen** Sie müssen in der Lage sein, mit externen Kunden über Service Level Agreements (SLA) und mit internen Kunden über Operational Level Agreements (OLA) oder auf einem weniger formellen Wege zu kommunizieren. Sie müssen technisch sowie geschäftsorientierten Benutzern bei der Einschätzung helfen, ob das Netzwerk zur Unterstützung des Unternehmens geeignet ist. Darüber hinaus müssen sie die wesentlichen Ursachen von Problemen erkennen und aufzeigen können.

Die CA-Lösung für Netzwerk- und Sprachmanagement

Die CA-Lösung für Netzwerk- und Sprachmanagement ermöglicht Ihnen ein konvergentes Sprach- und Datenmanagement. Die Lösung erfüllt die Anforderungen an die IT hinsichtlich einer proaktiven Verwaltung von End-to-End-Sprach- und -Datendiensten, sorgt für ausreichende Bandbreite und Systemkapazitäten und unterstützt die vom Unternehmen definierten Service-Level. Die Lösung ist ein zentraler Bestandteil des Enterprise IT Management (EITM). Dieses spiegelt die Unternehmensvision von CA, wie IT-Umgebungen dynamisch verwaltet und gesichert werden können, damit Unternehmen das volle Potenzial der bereitgestellten IT ausschöpfen können, wider.

Die CA-Lösung für Netzwerk- und Sprachmanagement beinhaltet sowohl IP- als auch herkömmliche Sprachtechnologien. Auf diese Weise können die Unternehmen selbst entscheiden, wann sie auf die IP-Telefonie migrieren. Darüber hinaus wird die Komplexität bei der Verwaltung heterogener Infrastrukturen verringert.

Die getestete integrierte Lösung bietet folgende wesentliche Merkmale:

- **Effektives Service-Level-Management** ermöglicht die Festlegung von Baselines sowie die Bewertung und Verfolgung von Services innerhalb des gesamten Netzwerks und hält Techniker und Unternehmen über die Erfüllung von SLAs und OLAs auf dem Laufenden.
- **Proaktive Sicherung von Services** spürt mit Hilfe einer richtlinienbasierten Überwachung Serviceleistungsabfälle auf, bevor sich diese auf Kunden oder Endbenutzer auswirken.
- **Schnelle Problemerkennung** löst die eigentliche Ursache von Problemen durch Ereigniskorrelation, Ursachenanalyse (Root Cause Analysis, RCA) und Verknüpfung von Echtzeit- und historischen Berichten.
- **Vorausschauende Kapazitätsplanung** verwendet intelligente integrierte Algorithmen, auf deren Basis die Netzwerkmanagementteams ermitteln können, wann und wo Änderungen an Schaltungen oder Hardware erforderlich sind, damit der Service weiterhin innerhalb der erwarteten Leistungsschwellenwerte liegt.

Die CA-Lösung für Netzwerk- und Sprachmanagement besteht aus drei Hauptkomponenten, die gemeinsam ein konsistentes Paket von Funktionen für die gesamte Sprach- und Infrastruktur bereitstellen.

- **eHealth Network Performance Management** sammelt und speichert die leistungskritischen Daten von über 100 Herstellern und mehr als 1000 Geräten; wendet intelligente Algorithmen auf die Leistungsdaten an, um Serviceleistungsabfälle, Probleme bei der Kapazitätsplanung sowie die Ursachen von Leistungsproblemen zu ermitteln.
- **SPECTRUM Fault Management** umfasst Fehler-Management, RCA und Service Level-Management.
- **eHealth for Voice** ermöglicht die Verwaltung von Systemleistung und Fehlern auf herkömmlichen TDM- und IP-Kommunikationssystemen, Messaging-Systemen und TK-Anlagen (PBX).

Mit dieser leistungsstarken und einzigartigen Lösung können die zunehmend komplexeren Netzwerkservices von Unternehmen, Behörden und Telekommunikationsumgebungen optimal verwaltet werden. Die Lösung bietet Technikerteams Unterstützung bei der Optimierung von Services, der Kontrolle von Kosten, der Senkung von Risiken und der Erhöhung der Rentabilität, wenn die IT-Infrastruktur als Unternehmensdienstleistung eingesetzt wird.

Um eine erfolgreiche Implementierung zu gewährleisten, unterstützt CA Technology Services™ Unternehmen bei der Bewertung, Entwicklung, Implementierung und Optimierung von Netzwerkleistungs- und -verfügbarkeitslösungen. Die Implementierung der Gesamtlösung des Netzwerkmanagements basiert auf einem Ansatz, der folgende Aspekte des Lebenszyklus berücksichtigt:

■ **Bewertung** Lücken erkennen

Umfassende Bewertungen, z. B. das so genannte Event-to-Resolution Readiness Assessment, mit denen der aktuelle Stand und die Effizienz von Netzwerkleistung und Verfügbarkeitsmanagement bewertet werden.

■ **Entwurf** Die geeignete Lösung entwickeln

Die Architekten von CA entwerfen für Kunden bewährte Serviceverfügbarkeitslösungen mit variablem Umfang, angefangen bei Einzelstandorten über mittelständische Unternehmen bis hin zu globalen IT-Unternehmen, die rund um die Uhr verfügbar sein müssen und eine entsprechende Hochgeschwindigkeitsleistung benötigen.

■ **Implementierung** Die Basis für den Erfolg der Lösung

Die CA-Berater richten die Umgebung ein, installieren, konfigurieren und passen Ihre eHealth- und SPECTRUM-Lösungen an, überprüfen und dokumentieren die eHealth- und SPECTRUM-Lösungen auf Test-, Qualitätssicherungs- und Produktionssystemen und vermitteln Ihrem Personal die notwendigen Kenntnisse.

■ **Optimierung** Den richtigen Zeitpunkt für Änderungen erkennen

Mit Hilfe von Optimierungsservices wird ermittelt, inwiefern die eingesetzten eHealth- und SPECTRUM-Lösungen noch besser ausgelastet und auf Ihre Anforderungen abgestimmt werden können. Zum Serviceumfang der eHealth-Prüfung gehören die Anpassung, Neukonfiguration, Aktualisierung, Migration sowie Schulungen und Zertifizierungen.

Mit der CA-Lösung für konvergentes Netzwerk- und Sprachmanagement wählen Sie die proaktive – und nicht die reaktive – Strategie des Sprach- und Datenmanagements. Netzwerkteams verfügen über Tools, mit denen Probleme und deren Ursachen umgehend identifiziert werden können. Die Abteilung für IT-Planung und -Entwicklung kann feststellen, ob die eingesetzten Ressourcen nicht genügend ausgelastet werden oder an Leistungsgrenzen stoßen. Die IT-Abteilung kann den Kontakt zu Entscheidungsträgern mit Hilfe von formalen Service-Levels verwalten. Die Möglichkeit, die Größen GoS (Grade of Service) und QoS (Quality of Service) für Anrufe im Sprachnetzwerk zu überwachen und zu protokollieren, bildet eine wesentliche Voraussetzung für das erfolgreiche Service-Level-Management. Die CA-Lösung für Netzwerk- und Sprachmanagement wird allen der genannten Anforderungen gerecht.

Kapitel 2: Herausforderungen beim Netzwerk- und Sprachmanagement

Jedes Rechnersystem – Großrechner, Client-Server, verteilte Systeme, Grid-Systeme, Web-Service-EDV – ist von der Arbeitsweise des Netzwerks abhängig, in dem es sich befindet. Die Unternehmen von heute haben erkannt, dass die für den Geschäftserfolg entscheidenden Services, z. B. Anwendungen für Finanzbuchhaltung oder Sprache, von der Infrastruktur des Netzwerks abhängig sind. Wenn die Infrastruktur ausfällt oder zu langsam arbeitet, wirkt sich dies auf die geschäftskritischen Anwendungen und Services aus, sowie auf die Endbenutzer, die auf deren Verfügbarkeit angewiesen sind. Dies führt zu Einbußen in Umsatz und Produktivität und lässt gleichzeitig die Kosten ansteigen. Nach Einschätzung von Infonetics kosten solche Ausfallzeiten und Leistungsabfälle der Infrastruktur die Unternehmen im Durchschnitt bis zu 3,6 % ihrer jährlichen Erträge.¹

Entwicklung von der reinen Netzwerkdienstleistung zur Serviceimplementation

Innerhalb der letzten Jahre hat sich die Funktion von Netzwerken stark gewandelt. Dieser Wandel hat nicht nur bedeutsame Auswirkungen auf die Netzwerkmanagement-Software und die Arbeitsabläufe, sondern auch auf die Mitarbeiter der IT-Teams, die täglich damit arbeiten. Noch vor nicht allzu langer Zeit bestand die Hauptaufgabe von Netzwerken darin, die Konnektivität der Daten zu gewährleisten.

Heutzutage werden Netzwerke eher als Plattform zur Bereitstellung von Services betrachtet. Netzwerke unterstützen Echtzeit-Services wie Voice over IP (VoIP), IP Television (IPTV) und Videokonferenzen, die sich seit den Anfängen weiterentwickelt haben und nun in zunehmendem Umfang eingesetzt werden. Unternehmen sind immer mehr auf Anwendungen angewiesen, die über große geografische Regionen hinweg bereitgestellt werden und Mitarbeitern, Kunden und Partnern jederzeit Zugriff gewähren, damit sie die für das Unternehmen wichtigen Aufgaben ausführen können. Darüber hinaus werden die Komponenten, aus denen moderne Netzwerke bestehen, heutzutage mit Services wie Sicherheit, hohe Verfügbarkeit und Speicher integriert, die bis vor kurzem in Infrastrukturen außerhalb des Netzwerks ausgelagert wurden.

¹Infonetics Research, *The Cost of Enterprise Downtime, North America 2004*.
<http://www.infonetics.com>. Verwendung mit Einverständnis von Infonetics.

Auswirkungen auf die Netzwerkteams

Diese Entwicklung hat maßgeblichen Einfluss auf die Rollen und Zuständigkeiten der Netzwerkteams. Da die Unternehmen zur Steigerung ihrer Erträge und Produktivität und zur Senkung ihrer Kosten auf Echtzeit-Services angewiesen sind, wirken sich Serviceleistungsabfälle sofort nachteilig auf die Kundenzufriedenheit und das Unternehmen aus.

Da im Netzwerk Anwendungen eingesetzt werden, die sich unmittelbar auf die Bilanz des Unternehmens auswirken, sind nicht nur Techniker, sondern auch andere Gruppen im Unternehmen, z. B. nicht im technischen Bereich tätige, geschäfts- und branchenorientierte Mitarbeiter, an der Funktionsweise und Performance des Netzwerks interessiert. Die Mitarbeiter von Netzwerkteams sehen sich nun einer ganz neuen Gruppe interner und externer Auftraggeber gegenüber, denen sie die Erfüllbarkeit von Service-Level-Verpflichtungen vermitteln müssen. Da diese Personengruppe nicht im technischen Bereich tätig ist, sollten hierbei betriebswirtschaftliche Fachbegriffe verwendet und technische Details ausgespart werden.

Aufgrund der engen Verflechtung zwischen der Netzwerkinfrastruktur und den Anwendungen und Services, die über diese Infrastruktur bereitgestellt werden, müssen die Netzwerkteams nun nicht mehr nur die Netzwerkinfrastruktur beaufsichtigen, sondern auch Anwendungen, Sprache und andere Services. Dieser Zuwachs erfordert ein tieferes Verständnis der neuen Technologien, für die in der Vergangenheit andere Teams zuständig waren. Durch die Einbettung der Services in die Netzwerkkumgebung haben sich die Anzahl und die Komplexität der von den Netzwerkteams verwalteten Geräte erhöht. Im Zuge dessen sind die Anforderungen an die Teams noch weiter gewachsen.

Änderung der Anforderungen an die Netzwerkmanagement-Software

Die neuen Herausforderungen, die mit der Entwicklung konvergenter Netzwerke und Netzwerkprozesse einhergehen, erfordern Management-Lösungen, die kontinuierlich die Verbindung zwischen dem Unternehmen und seinen externen und internen Kunden aufrechterhalten. Der strategische Einsatz der Netzwerkmanagement-Funktionen trägt dazu bei, dass Probleme der Zuständigkeit zwischen Netzwerk-, Anwendungs- und IT-Verwaltern reduziert werden. Während sich die eine Gruppe um Fragen der Netzwerkleistung kümmert, ist die andere dafür verantwortlich, dass die im Netzwerk bereitgestellten Anwendungen funktionstüchtig sind und die internen Kunden mit der Arbeitsweise dieser Anwendungen zufrieden sind.

Ein weiterer wesentlicher Bestandteil ist die umfangreiche Auswahl an Berichten und Statistiken, mit denen der Status des Netzwerks dokumentiert wird. Einfache und benutzerfreundliche Netzwerkmanagement-Tools – mit übergeordneten Alert-Dashboards und Funktionen, die den Benutzern helfen, ihre Anwendungs- und Netzwerkprobleme einzugrenzen – finden zunehmend stärkere Resonanz und werden sich letztlich auch im IT-Etat niederschlagen.

Der Einsatz konvergenter Netzwerke sowohl in Unternehmen als auch bei Serviceanbietern macht es erforderlich, dass Netzwerkverwalter und IT-Mitarbeiter die Netzwerkbedingungen für alle Anwendungen und Abläufe getrennt prüfen. In drahtlosen lokalen Netzwerken (WLAN) werden bereits neue Verfahren zum Management von Netzwerk, Sicherheit und VoIP sowie zur Konfiguration von Netzwerken eingesetzt. Automatisierungs- und Visualisierungstools für Serviceanbieter gewinnen insbesondere dann an Bedeutung, wenn Services über mehrere Netzwerke und für mehrere Standorte bereitgestellt werden sollen. Dieser Bedarf wird durch die kompakt strukturierte Logistikkette in Informationsnetzwerken sowie den wachsenden Trend zum verteilten und mobilen Einsatz von Arbeitskräften noch weiter verstärkt.

Die mit der Verwaltung konvergenter Netzwerke beauftragten Betreiberteams sehen sich mit folgenden entscheidenden Herausforderungen konfrontiert:

- **Heterogene Netzwerke** In heutigen Netzwerken wird ein breites Spektrum an Technologien verschiedener Hersteller eingesetzt, z. B. Technologien zur Datenübertragung wie IP, ATM, FR und Breitbandverfahren sowie Sprachinfrastrukturen, die sich aus herkömmlichen TDM-Infrastrukturen, speziellen IPT- und hybriden Infrastrukturen zusammensetzen. Die Migration auf VoIP wird in der Regel schrittweise vollzogen. Daher müssen herkömmliche TDM-Umgebungen und Umgebungen mit IP-Telefonie häufig noch parallel verwaltet werden.
- **Skalierung** Die modernen Sprach- und Dateninfrastrukturen verfügen über eine große Reichweite und erstrecken sich über große geografische Regionen – über Zeitzonen, Länder und sogar Kontinente. Zur Unterstützung derart umfangreicher Infrastrukturen muss das Management-System skalierbar sein, und für die Betreiberteams, egal ob auf zentraler oder regionaler Ebene, müssen alle erforderlichen Informationen bereitgestellt werden.
- **Anforderungen an die Verwaltung von Dateninfrastrukturen, Sprachinfrastrukturen und kritischen Systemen** Das Management-System muss domänenübergreifend eingesetzt werden, damit die Mitarbeiter des IT-Teams auch technische Domänen, die bis vor kurzem als Silos verwaltet wurden, problemlos verwalten können.
- **Anforderungen an die Übermittlung der QoS an verschiedene Personengruppen** Die Betreiberteams müssen sich externen Kunden über SLAs und internen Kunden über OLAs oder auf einem weniger formellen Weg mitteilen können. Die Management-Software muss daher die Informationen und Funktionen bereitstellen, um für technische und geschäftsorientierte Benutzer folgende Aufgaben auszuführen:
 - > Einschätzung, ob die Infrastruktur zur Unterstützung des Unternehmens geeignet ist
 - > Identifizierung der auftretenden Probleme
 - > Eingrenzung der Quellen und Ursachen für Probleme

Eine Folge dieser Trends ist das rapide Marktwachstum im Bereich der weltweit verfügbaren Netzwerklösungen. Durch den Einsatz effektiver Netzwerkmanagement-Software verfügen die Unternehmen über die notwendigen Tools, um leistungsfähigere Strukturen zu entwickeln.

(Diese Seite wurde absichtlich leer gelassen)

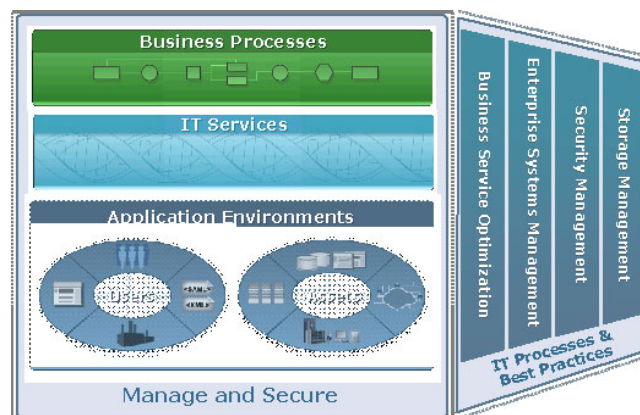
Kapitel 3: Die CA-Lösung für Netzwerk- und Sprachmanagement

EITM: Die Unternehmensvision von CA

EITM spiegelt die Unternehmensvision von CA, wie IT-Umgebungen dynamisch verwaltet und gesichert werden können, damit Unternehmen das gesamte IT-Potenzial zum Vorteil des Unternehmens ausschöpfen können, wider. EITM bildet die allgemeine Grundlage für die Integration und gemeinsame Nutzung von Services und Daten. Dank EITM können alle IT-Assets und -Ressourcen (Infrastruktur, Anwendungen und Geschäftsprozesse) zentral koordiniert und aufeinander abgestimmt werden. Dieser unternehmensorientierte Ansatz bietet auch die Möglichkeit, die Verwaltung von Netzwerken, Systemen, Speichermedien, Datenbanken, Anwendungen und Sicherheit zu integrieren, und stellt modernste Methoden bereit, mit denen der Einfluss der IT auf Unternehmensziele gemessen, optimiert und dokumentiert werden kann.

CA ist weltweit Marktführer bei der Entwicklung von Management-Software. Wir sind nunmehr seit drei Jahrzehnten in dieser Branche tätig und haben uns auf die Entwicklung von Lösungen für alle Bereiche des Infrastrukturmanagements spezialisiert. Wir betrachten es als unsere Aufgabe, Unternehmen bei der Erfüllung ihrer Ziele zu unterstützen, indem wir dazu beitragen, die IT-Kosten zu senken und die Kapitalkosten und anderen betrieblichen Ausgaben zu optimieren, Risiken zu verringern und Bestimmungen zu erfüllen. Wir stellen sicher, dass die Infrastruktur zu jeder Zeit die volle Leistung liefert.

Der Kern des CA-Ansatzes besteht in der Entwicklung von Management-Lösungen, die eine vereinheitlichte Sicht auf die Assets und Vorgänge des Unternehmens bieten und deren Verknüpfung mit geschäftlichen Aktivitäten und Anforderungen aufzeigen. Diese Sicht ermöglicht es Unternehmen, die eingesetzte IT mit den geschäftlichen Anforderungen zu koordinieren und bei der Ausrichtung ihrer geschäftlichen Aktivitäten und der Nutzung ihrer Assets bessere, sachkundigere Entscheidungen zu treffen.



Ein Merkmal der Management-Lösungen von CA ist die Serviceverfügbarkeit, die dafür sorgt, dass IT-Abteilungen permanent hochwertige IT-Services bereitstellen können. Die Grundlage dafür bildet das proaktive integrierte Management, das einen Einblick in den Zustand der Systeme und Anwendungen bietet, von denen die Unternehmensservices abhängen.

Enterprise Systems Management

Parallel zu den Bestrebungen der Unternehmen, ihren geschäftlichen Einfluss auszuweiten, um größere Zielgruppen zu erreichen und noch wettbewerbsfähiger zu werden, hat sich eine neue Generation von Lösungen für das Netzwerk- und Systemmanagement herausgebildet, die die Unternehmen dabei unterstützen soll, bei der Optimierung der Leistung und Verfügbarkeit ihrer Geschäftsprozesse einen proaktiveren und stärker serviceorientierten Ansatz zu verfolgen. Durch den Einsatz dieser Lösungen können Risiken verringert oder zumindest abgeschwächt werden. Im selben Maße können die betriebliche Auslastung, die geschäftliche Kontinuität und die Erfüllung gesetzlicher Vorschriften optimiert werden. Das Ergebnis ist eine rentable IT-Umgebung, die auf das Unternehmen abgestimmt ist.

Die Lösungen für das Enterprise Systems Management sind so flexibel und leistungsfähig, dass bei allen bereitgestellten IT-Services die Anforderungen und Bedingungen des Unternehmens im Vordergrund stehen. Diese Management-Lösungen müssen so angelegt sein, dass allen Geschäftsanforderungen je nach ihrer Bedeutung für das Unternehmen IT-Ressourcen zugeordnet werden können. Eines der wichtigsten Merkmale der Enterprise Systems Management-Lösungen von CA ist die Automatisierung, die auf Basis festgelegter Richtlinien erfolgt.

Die Hauptaufgabe der eingesetzten IT besteht in der Aufrechterhaltung des reibungslosen Betriebs mit funktionstüchtigen Services, die mit hoher Verfügbarkeit und Leistung bereitgestellt werden. Um diese Ziele zu erfüllen, werden mit Hilfe der CA-Lösungen für das Enterprise Systems Management folgende Leistungen sichergestellt:

- Netzwerke und Systeme werden hinsichtlich Verfügbarkeit und Leistung vernünftig verwaltet.
- Jobs und Ereignisse werden mit Hilfe von Automatisierungen optimiert.
- Anwendungen und Datenbanken werden im Hinblick auf die Leistung verwaltet.
- Desktops und Server werden eingerichtet und konfiguriert.

CA ist sich bewusst, dass das Enterprise-Management nicht losgelöst von anderen Komponenten betrachtet werden kann. Es bildet einen Bestandteil einer übergreifenden IT-Infrastruktur, mit der verschiedene Bereiche abgedeckt werden. Server sind nur dann wirklich von Nutzen, wenn sie innerhalb hochleistungsfähiger Netzwerke zuverlässig ihren Dienst verrichten können. Auch Anwendungen sind nur so sicher wie die Systeme, die ihren Zugriff kontrollieren. Und nicht zuletzt ist der Betrieb auch davon abhängig, dass die verwendeten Speichersysteme den geschäftlichen Anforderungen genügen.

Die Vision von CA beruht auf der Überzeugung, dass Bereiche, die traditionell als eigenständig betrachtet werden – Netzwerke und Systeme, Speicher, Sicherheit und Servicemanagement – stärker verknüpft werden sollten, um so die Leistung, Zuverlässigkeit und Produktivität der IT-Umgebungen in Unternehmen zu optimieren. CA hat Produkte entwickelt, die miteinander interagieren. Die gemeinsamen Softwarekomponenten von Services werden dazu eingesetzt, wiederverwendbare und anwendungsübergreifende Funktionen auszuführen. Mit der Entwicklung einer zentralen Managementdatenbank, die eine vereinheitlichte Sicht auf die verschiedenen Bereiche und die damit verbundenen Aktivitäten und Anforderungen des Unternehmens bietet, hat CA die Grundlage für eine auf das Unternehmen konzentrierte Ausrichtung der IT-Umgebung geschaffen.

Durch den Zugriff auf umfassende und bereichsübergreifende Informationen erhalten IT-Organisationen einen vollständigen Überblick darüber, wie die einzelnen IT-Ressourcen in ihren Unternehmen eingesetzt werden. Mit diesem Wissen können IT-Organisationen das Serviceangebot auf die speziellen Anforderungen der einzelnen Abteilungen abstimmen und Entscheidungsträgern Rückmeldung geben, wie die IT-Ressourcen eingesetzt werden und welche Kosten dabei entstehen. Dadurch wird auch die Position der Entscheidungsträger gestärkt, die auf Basis dieser Informationen sachkundigere Entscheidungen zur Ausrichtung ihrer geschäftlichen Aktivitäten treffen können.

Mehrwert der CA-Lösung für Netzwerk- und Sprachmanagement

Die Wettbewerbsfähigkeit moderner Unternehmen ist stark abhängig von hochwertigen Sprach- und Datenlösungen. Die CA-Vision eines konvergenten Sprach- und Datenmanagements unterstützt die häufig an IT-Lösungen gestellte Anforderung eines proaktiven End-to-End-Managements von Sprach- und Datenservices, stellt eine ausreichende Bandbreite und Systemleistung sicher und unterstützt die vom Unternehmen definierten Service-Level. Die CA-Lösung für Netzwerk- und Sprachmanagement beinhaltet sowohl IP- als auch herkömmliche Sprachtechnologien. Auf diese Weise können Unternehmen selbst entscheiden, wann sie auf die IP-Telefonie migrieren, und die Komplexität bei der Verwaltung ihrer heterogenen Infrastrukturen verringern. Unsere Produktstrategie unterstützt diese Vision durch regelmäßige Aktualisierungen, Neuerungen und Integration auf der Grundlage der Anforderungen unserer Kunden.

Die CA-Lösung für Netzwerk- und Sprachmanagement bietet folgende wesentliche Vorteile:

- **Effektives Service-Level-Management** Die Lösung ermöglicht die Festlegung von Baselines sowie die Bewertung und Verfolgung von Services innerhalb des gesamten Netzwerks und hält Techniker und Unternehmen über die Erfüllung von SLAs und OLAs auf dem Laufenden.
- **Proaktive Servicesicherung** Die Lösung verfolgt einen richtlinienbasierten Ansatz zur Überwachung eines Abfallens der Serviceleistung und bietet die Möglichkeit, Leistungsabfälle rechtzeitig zu erkennen, bevor sie sich auf den Kunden auswirken, und diese in RCA und Ereigniskorrelation zu berücksichtigen.
- **Schnelle Problemerkennung** Die Hauptaufgabe der Lösung besteht in der Erkennung der eigentlichen Ursachen von Problemen durch Ereigniskorrelation, Ursachenanalyse (Root Cause Analysis, RCA) und Verknüpfung von Echtzeit- und historischen Berichten.

- **Vorausschauende Kapazitätsplanung** Die Grundlage der Lösung bilden intelligente integrierte Algorithmen, anhand derer die Netzwerkteams ermitteln können, wann Up- oder Downgrades an Schaltungen oder anderer Hardware erforderlich sind. Diese Entscheidungen sind sowohl von den Nutzungstrends in der Vergangenheit als auch den jeweiligen Schwellenwerten abhängig.

Unsere Netzwerk- und Sprachmanagement-Strategie verfolgt vier Ziele:

- Unseren Kunden soll ermöglicht werden, ihre Geschäftsprozesse sowie ihre Daten-, Sprach- und Multimediasdienste entsprechend ihrer Wettbewerbsstrategie zu verwalten.
- Unseren Kunden soll ermöglicht werden, ihre konvergenten Netzwerke und die darin eingesetzten geschäftskritischen Anwendungen zu verwalten und den Wechsel auf die IP-Telefonie zu vollziehen.
- Mit den Lösungen soll ein End-to-End-Fehler- und Leistungsmanagement für Daten und Sprache (TDM und IP-Telefonie) sowie für System- und Anwendungsinfrastrukturen bereitgestellt werden.
- Das Management soll auf Sprach- und Multimediaressourcen sowie die Infrastruktur des Netzwerks ausgeweitet werden.

CA ist der einzige Hersteller, der Ihnen folgende Leistungen bieten kann:

- Eine integrierte, proaktive Management-Lösung
- Eine Lösung, die sowohl IP- als auch herkömmliche Technologien unterstützt
- Lösungen, die vor, während und nach der Migration auf VoIP die volle Funktionsfähigkeit des Sprachnetzwerks garantieren.

Mit der CA-Lösung für konvergentes Netzwerk- und Sprachmanagement wählen Sie die proaktive – und nicht die reaktive – Strategie des Sprach- und Datenmanagements. Statt passiv zu bleiben und abzuwarten, bis sich die Kunden über die geringe Sprachqualität beschweren, werden die IT-Mitarbeiter umgehend informiert, wenn Richtlinien zu Schwankungen, MOS (Mean Opinion Score) oder Hardwareproblemen, z. B. T1-Leitungen, benutzerdefinierte Schwellenwerte überschreiten. Bei Problemen, die in IP-Telefonie-Umgebungen auftreten, sind die Ursachen manchmal schwer zu bestimmen. Es kommt beispielsweise vor, dass sich ein Benutzer beschwert, dass er einen bestimmten Anruf nicht tätigen konnte. Viele Alarmereignisse können jedoch von Routern, IPT-Systemen, Anlagen usw. verursacht werden. Die CA-Lösung für Netzwerk- und Sprachmanagement bietet einen proaktiven Ansatz zur Verwaltung von IP-Telefonie und VoIP.

Die Kapazitätsplanung bildet eine wichtige Voraussetzung für das konvergente Sprach- und Datenmanagement. Anhand der Daten, die von Sprachsystemen, sowohl herkömmlichen als auch IPT-Systemen, und vom Netzwerk (einschließlich der Kapazität von Verbindungen und Anschlüssen) erhoben werden, können IT-Techniker erkennen, wann nicht ausgelastete Ressourcen einen Schwellenwert erreicht haben. Diese Informationen können dann als Grundlage für die vorausschauende Kapazitätsplanung des gesamten Netzwerks dienen. IT-Abteilungen haben die Aufgabe, Service-Levels für die Hauptzielgruppen bereitzustellen, wozu insbesondere umsatzgenerierende Geschäftseinheiten wie Kontaktcenter gehören. Eine weitere Voraussetzung für das Service-Level-Management bilden Funktionen, mit denen die Größen GoS und QoS für Anrufe im Sprachnetzwerk überwacht und protokolliert werden können.

Ein Schlüsselbestandteil der EITM-Vision von CA

Die CA-Lösung für Netzwerk- und Sprachmanagement fügt sich nahtlos in die unternehmensweite EITM-Strategie von CA ein. Die Lösung setzt die vier Hauptforderungen der IT-Vorstände in folgender Weise um:

- Mit Hilfe der proaktiven Servicesicherung werden Services verbessert und Probleme rechtzeitig erkannt, bevor sie sich auf die Endbenutzer auswirken. Leistungsfähige Tools wie RCA, Ereigniskorrelation und Folgenanalyse tragen dazu bei, dass die Infrastruktur des Netzwerks zuverlässig und reaktionsschnell arbeitet.
- Risiken werden durch Sicherung der geschäftlichen Kontinuität begrenzt, da die Unternehmen in die Lage versetzt werden, alle behördlichen und gesetzlichen Anforderungen zu erfüllen.
- Kosten werden dadurch beschränkt, dass die durch Ausfallzeiten (Ausfälle und Leistungsabfälle) verursachten Kosten drastisch gesenkt werden, weil Vorkommen und Dauer dieser Ausfallzeiten verringert werden.
- Die IT wird auf die Anforderungen des Unternehmens abgestimmt, indem das IT-Team einen Einblick in das Unternehmen, insbesondere den Status der End-to-End-Services des Unternehmens, erhält.

Netzwerk- und Sprachmanagement für die wichtigsten vertikalen Märkte

CA stellt eine leistungsfähige und einmalige Management-Software bereit, mit der die zunehmend komplexeren Netzwerkservices herkömmlicher Unternehmens- und Regierungsumgebungen sowie Telekommunikations-, Kabel- und mobile drahtlose Services sowie die Produkte anderer Serviceanbieter verwaltet werden können. Die Lösung bietet Technikerteams Unterstützung bei der Optimierung von Services, der Kontrolle von Kosten, der Senkung von Risiken und der Erhöhung der Rentabilität, wenn die IT-Infrastruktur als Unternehmensdienstleistung eingesetzt wird.

Serviceanbieter im Bereich Telekommunikation

CA sieht in den Anbietern von Telekommunikationsservices einen wichtigen vertikalen Markt, da deren Akteure die Betriebsumgebung als wesentliche Bedingung für die Begrenzung von Kosten und die Bereitstellung von Produkten/Differenzierung von Services betrachten. Diese Faktoren bilden die Voraussetzung, um mit den Herausforderungen moderner Telekommunikationsmärkte mithalten zu können.

Die meisten Serviceanbieter verwenden eine Auswahl von Management-Tools, die speziell auf das Element-Management, die Servicebereitstellung, die Abrechnung, den Kundenservice und die Servicesicherung zugeschnitten sind. Das hat zur Folge, dass in den Umgebungen großer Träger- und Serviceanbieter eine Vielzahl von Einzelanwendungen und Datenspeichern eingesetzt werden. Diese müssen irgendwie integriert werden, um daraus effiziente Arbeitsabläufe und Prozesse zu bilden, die sicherstellen, dass alle Services zuverlässig bereitgestellt werden und die Produktivität des Betriebs gewährleistet wird. Die CA-Lösung für Netzwerk- und Sprachmanagement bietet flexible Integrationspunkte, damit auch heterogene OSS-Softwareumgebungen (Operational Support System) erfolgreich verwaltet werden können. Gleichzeitig werden dadurch die für die Implementation benötigte Zeit und Komplexität sowie die Kosten für die Konfiguration und Wartung gesenkt. CA arbeitet mit zahlreichen führenden OSS-Herstellern in den Bereichen Servicesicherung, Auftragsabwicklung und Abrechnung/Kundenbetreuung zusammen.

Die CA-Lösung für das Netzwerk- und Sprachmanagement hilft Serviceanbietern bei der Erfüllung folgender Ziele:

- Prüfung und Bestätigung der Gewährleistung von SLAs, um die Kundenzufriedenheit zu erhöhen und den Wechsel zu anderen Anbietern zu verhindern.
- Senkung der Betriebsausgaben durch Verringerung der Ausfallzeiten sowie der durchschnittlichen Reparaturzeit (MTTR).
- Senkung der finanziellen Ausgaben durch intelligente Kapazitätsplanung.
- Beschleunigung des Supports für neue Serviceangebote:
 - > Virtuelles privates Netzwerk (VPN)
 - > VoIP
 - > Zusammenspiel von Sprache/Video/Daten
 - > Neue drahtlose Datenservices

Regierungen

Die CA-Software wird auch von Landesregierungen und örtlichen Behörden in hohem Umfang eingesetzt. Die CA-Lösung für Netzwerk- und Sprachmanagement erfüllt alle Anforderungen, die Zivil- und Verteidigungsbehörden an die Automatisierung von IT-Prozessen stellen. Sie bietet praktische, einsatzfähige Lösungen, die die Wertschöpfung beschleunigen und einen Einsatzerfolg garantieren. Wenn die Lösung auf Lastwagen oder anderen mobilen Fahrzeugen bereitgestellt wird, hat sie die Aufgabe sicherzustellen, dass die per IP, Satellit, Funk, Radar und Telefon geführte Kommunikation zuverlässig und mit der geforderten Leistung zwischen den Frontlinien und den Befehlshabern der verschiedenen Einsatzposten übermittelt wird. CA bietet einmalige Funktionen, um die Initiativen zur netzwerkzentrierten Kriegsführung zu unterstützen und die Möglichkeiten des Informationszeitalters auszuschöpfen.

Unternehmen

Die CA-Lösung für das Netzwerk- und Sprachmanagement wird auch innerhalb anderer vertikaler Märkte, z. B. in Automobilindustrie, Bildung, Energiewirtschaft, Unterhaltung, Konsumgüterindustrie, Finanzdienstleistung, Gesundheitswesen, Tourismusbranche, Versicherungsbranche, Fertigung, Pharmazie, Handel, Halbleitertechnik, Technik und Transportwesen, in großem Umfang eingesetzt. In allen diesen Branchen haben Ausfallzeiten verheerende Folgen.

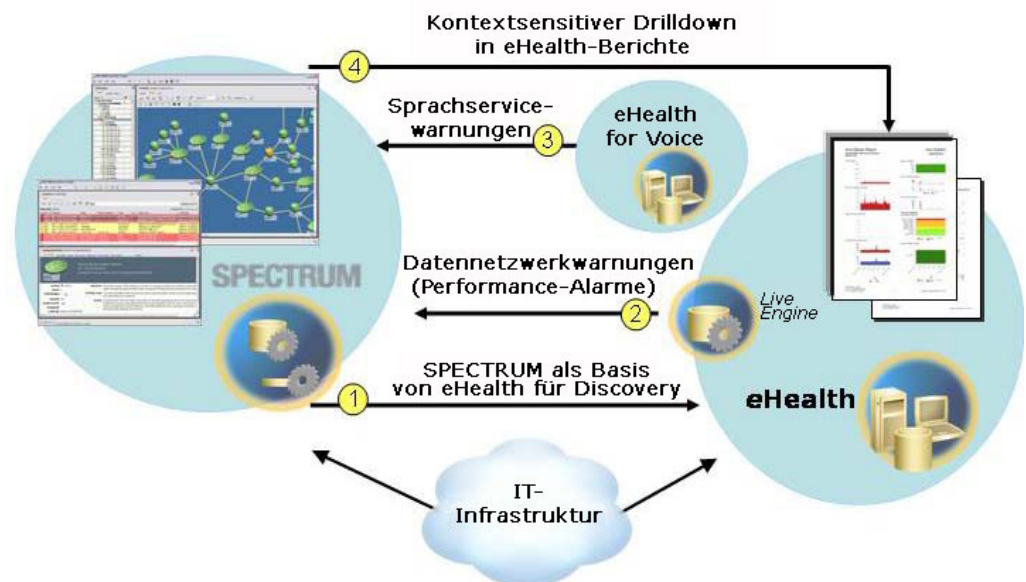
Um die Anforderungen an heutige konvergente Sprach- und Datennetzwerke zu erfüllen, müssen die Hauptkomponenten der entsprechenden Lösungen einerseits die End-to-End-Dateninfrastruktur und andererseits die bereitgestellten Voice-Messaging-Systeme und Services verwalten können. Diese Vielfalt an Infrastruktur kann nur mit Lösungen verwaltet werden, die Funktionen für das Leistungs- und Fehlermanagement sowie für das Sprachmanagement von PBX-, Messaging- und anderen Sprachservices enthalten. Darüber hinaus müssen sie eine Systemmanagementkomponente bereitstellen, damit die für den Netzbetrieb zuständigen Mitarbeiter kritische Systeme in eigener Verantwortung verwalten können.

Die Komponenten der Lösung

Die CA-Lösung für Netzwerk- und Sprachmanagement besteht aus drei Hauptkomponenten, die ein konsistentes Paket von Funktionen für die gesamte Sprach- und Dateninfrastruktur bilden:

- **eHealth** bewertet den Zustand des Netzwerks und überprüft, ob es für Sprache geeignet ist. Mit Hilfe dieser Komponente können Sie ablesen, wie zuverlässig das Netzwerk arbeitet, den MOS für Sprache mit den QoS-Statistiken vergleichen und Trends in der Leistung ermitteln.
- **SPECTRUM** stellt Komponenten für das Fehlermanagement, die Ursachenanalyse (RCA) und die Modellierung von Sprache bereit. Mit SPECTRUM können Sie auch die Komponenten Ihrer Sprachservices modellieren, um sicherzustellen, dass alle Services ordnungsgemäß ausgeführt werden.
- **eHealth for Voice** bietet Performance-Management für Kommunikations- (IP and Traditional TDM) und Messaging-Systeme und ermöglicht eine Verwaltung aus Telefonie-Perspektive.

Beide Anwendungen können eigenständig verwendet werden oder in bestehende Systeme integriert werden, wie weiter unten gezeigt wird.



eHealth

Mit Hilfe von eHealth können Sie die Netzwerkleistung kontrollieren und sicherstellen, dass die QoS innerhalb der gesamten Netzwerkinfrastruktur eingehalten wird. eHealth trägt zur erfolgreichen Ausführung einer Vielzahl von Aufgaben bei, z. B. zur Überprüfung der Verfügbarkeit und Leistung des Netzwerks, zur Dokumentation der Service-Levels, zur Verwaltung von Kapazitäten sowie zur detaillierten Planung der weiteren Entwicklung. Die Lösung hilft Ihnen bei der Bewältigung einer Reihe von Herausforderungen, wie der Verwaltung von Geräten verschiedener Hersteller, der Ermittlung von Quellen für Leistungsabfälle im Netzwerk, der Senkung häufig wiederkehrender WAN-Kosten (Wide Area Network) und der Bereitstellung konsistenter Berichte, die in der gesamten heterogenen Netzwerkinfrastruktur verfügbar sind.

Diese Komponente der Lösung hilft Ihnen bei der Erfüllung folgender Ziele:

- Verbesserung der Serviceverfügbarkeit im Netzwerk.
- Begrenzung der durch Ausfallzeiten bedingten Kosten sowie der Auswirkungen, die den Benutzern durch diese Ausfallzeiten entstehen.
- Schnellere Erkennung und Lösung von Problemen.
- Vorausschauende Planung von Kapazitäten.
- Verbesserung von QoS.
- Erfüllung und Bestätigung der vereinbarten Service-Levels.

Die eHealth-Komponenten

Zu eHealth gehören folgende Komponenten:

- eHealth E2E Console
- eHealth Live Health
- eHealth Traffic Accountant
- Report Center
- Distributed eHealth
- eHealth SPECTRUM Integration
- eHealth Universal Workflow Integration Modules (HP OpenView, IBM (Micromuse), Netcool, Cisco CIC)
- eHealth Universal Data Integration Modules (Cisco WAN Manager, Cisco IP Solution Center, Lucent, Nortel, Alcatel)
- eHealth Universal Wireless Integration Modules (Nortel, Starent)

Die Vorteile von eHealth

eHealth unterscheidet sich durch folgende Merkmale von anderen Lösungen:

- eHealth ermöglicht ein erstklassiges proaktives Management. Auf diese Weise können Probleme von der IT beseitigt werden, bevor sie sich auf die Erträge auswirken.
- eHealth kann mit mehr als 1000 Geräten von 100 verschiedenen Herstellern eingesetzt werden und bietet damit die umfangreichste Herstellerunterstützung.
- Die eHealth-Berichte enthalten genügend Informationen, um Probleme zu behandeln, ohne dass eine detaillierte Kenntnis der einzelnen Servicekomponenten erforderlich ist.
- eHealth unterstützt die Automatisierung von Baselines. Das bedeutet, eHealth lernt, wie sich die einzelnen Management-Einheiten im Normalfall verhalten. Allerdings bietet der Algorithmus „Abweichung von der Norm“ bezogen auf den Gesamtverlauf zuverlässigere Schwellenwerte, da der Vergleich auf einer kontinuierlichen Analyse basiert.

- Im Gegensatz zu CA verfügen viele Hersteller lediglich über ein begrenztes Angebot an unterstützten Geräten und Technologien. Das ist insbesondere für die Unternehmen ein Problem, die ihre Management-Software von einer überschaubaren Anzahl von Herstellern beziehen wollen.
 - > Da die eingesetzte IT immer stärker die Funktion eines Services einnimmt, wünschen sich die Kunden mehr Verantwortung von den Herstellern.
 - > Eine kleinere Anzahl von Herstellern führt zur Verringerung der Komplexität, zur Optimierung der Betriebsausgaben sowie zur Senkung von Risiken, indem neue Geschäftsinitiativen eingeführt werden.
- Der durch eine integrierte Managementplattform erzielte Wertzuwachs ist enorm, da die IT-Operationen, die zur Ermittlung von Problemursachen eingesetzt werden, eine Menge Zeit und Geld erfordern und Ausfallzeiten zudem extrem hohe Kosten verursachen.

SPECTRUM

Mit SPECTRUM kann sowohl das lokale Netzwerk von nebenan als auch das global operierende Netzwerk verwaltet werden. SPECTRUM bietet Sichtbarkeit innerhalb der granularen Schichten 2 und 3 bis hin zu den Einzelanschlüssen und -leitungen von lokalen Netzwerken (LAN), WANs, verdrahteten, drahtlosen, physischen und virtuellen Netzwerken. Es stellt spezielle Managementanwendungen bereit, mit denen die Funktionsweise von ATM, Frame Relay, IP Multicast, QoS, Sprache und VPN überwacht und analysiert werden kann. Durch den Einsatz der patentierten Ursachen- und Folgenanalyse können Serviceausfälle und Leistungsabfälle genau lokalisiert werden.

Diese Komponente der Lösung hilft Ihnen bei der Erfüllung folgender Ziele:

- Verwaltung der Serviceverfügbarkeit im Netzwerk.
- Ermittlung der Ursachen von Netzwerkfehlern.
- Anzeigen der Beziehungen und Wechselwirkungen zwischen der IT-Infrastruktur und den Unternehmensservices.
- Überprüfung von Personal und Status, die bestimmten Vorgängen zugewiesen sind.
- Sicherung der operativen Integrität der Infrastruktur, indem alle Änderungen der Infrastruktur verfolgt werden.

Die SPECTRUM-Komponenten

Zu SPECTRUM gehören folgende Komponenten:

- SPECTRUM Infinity
- SPECTRUM Integrity
- SPECTRUM Xsight
- SPECTRUM OneClick
- SPECTRUM Service Manager
- SPECTRUM Report Manager
- SPECTRUM Alarm Notification Manager
- SPECTRUM ATM Circuit Manager
- SPECTRUM Configuration Manager

- SPECTRUM Secure Domain Manager
- SPECTRUM Frame Relay Manager
- SPECTRUM Microsoft Operations Manager Connector
- SPECTRUM Multicast Manager
- SPECTRUM OSS Integrations
- SPECTRUM QoS Manager
- SPECTRUM Remedy ARS Gateway
- SPECTRUM SNMPv3 Support
- SPECTRUM VPN Manager
- SPECTRUM Watch Editor
- SPECTRUM Service Performance Manager

Die Vorteile von SPECTRUM

SPECTRUM unterscheidet sich durch folgende Merkmale von anderen Lösungen:

- SPECTRUM bietet eine erstklassige Ursachenanalyse (RCA) und ermöglicht den Zugriff auf die Wissensbasis der SPECTRUM-Lösung:
 - > Es wird weniger Zeit benötigt, um die Ursachen von IT-Problemen zu ermitteln.
 - > Es wird weniger Zeit verschwendet, um falschen Alarmen und Alerts nachzugehen.
 - > Probleme der Zuständigkeit und die Verweigerung von Rechenschaft werden künftig ausgeschlossen.
- Die eingesetzte IT kann nach wie vor von der erweiterten RCA mit regelbasiertem Ereignis-Management-System (EMS) oder richtlinienbasierter Bedingungskorrelation (keine modellbasierte IMT (Inductive Modeling Technology)) profitieren.
- Dank intelligenter Schwellenwerte werden Probleme schon beim ersten Anzeichen erkannt und verhindert. In anderen Lösungen werden Probleme erst erkannt, nachdem sie bereits aufgetreten sind.

Integration von eHealth and SPECTRUM

Durch die Integration von eHealth und SPECTRUM werden die Vorzüge von Netzwerkfehler- und Leistungsmanagement in einer gemeinsamen Lösung kombiniert. Dadurch wird sichergestellt, dass Ihre geschäftskritischen Datennetzwerke stets verfügbar sind und auf alle Anfragen reagieren. Die Integration bietet den Kunden folgende Funktionen:

- Live Health-Alarme sowie Ausnahmealarme von Health-Berichten werden in SPECTRUM integriert und anschließend in der OneClick-Schnittstelle von SPECTRUM angezeigt.
- Die Alarm- und Topologieansichten von SPECTRUM können je nach Kontext in eHealth-Berichten aufgerufen werden.
- Bestimmte von SPECTRUM bereitgestellte Dateien können für die eHealth-Discovery eingesetzt werden.

eHealth for Voice

eHealth for Voice ermöglicht eine umfassende Verwaltung der Sprachservices im gesamten Netzwerk, z. B. die Nutzung von PBX, IP-Telefonie, Voice Messaging, Unified Messaging und Bandbreite.

Diese Komponente der Lösung hilft Ihnen bei der Erfüllung folgender Ziele:

- Konsolidierung der Informationen von verschiedenen Systemen und Netzwerkkomponenten (sowohl herkömmlichen als auch IP-basierten). Auf diese Weise erhalten Sie einen umfassenden Überblick über das Sprachsystem und die Netzwerkleistung.
- Automatisierung von Datensammlungs- und Pollingprozessen, um per Modem, IP oder Systemen mit sicherem Zugriff Daten von herkömmlichen Geräten abzurufen.
- Identifizierung von Komponenten der IP-Telefonie-Infrastruktur.
- Verwaltung der QoS-Richtlinien zur Übertragung von Sprache.
- Überwachung von Sprach-Gateways, digitalen Signalprozessoren (DSP) und Peer-to-Peer-Verknüpfungen.
- Abschätzung der MOS-Werte zwischen Router-Endpunkten.
- Durchgängige Sichtbarkeit von Sprachqualität, Jitter und Verzögerungen.

eHealth for Voice bietet Ihnen einen umfassenden Überblick über Sprachsysteme, Netzwerke und Services, damit Sie Ihre Service-Levels effektiv verwalten und bis ins Detail analysieren können. Nur so können Sie sicherstellen, dass Kapazitäten, RCA und proaktive Servicesicherung in ausreichendem Umfang verfügbar sind.

Die Vorteile von eHealth for Voice

eHealth for Voice bietet folgende Vorteile:

- Mit eHealth for Voice können Sie Geschäftsprozesse wie Sprach- und Multimedia-Services entsprechend Ihrer Wettbewerbsstrategie verwalten.
- eHealth for Voice hilft Ihnen beim Wechsel von herkömmlicher auf IP-Telefonie.
- eHealth for Voice ermöglicht ein durchgängiges Fehler- und Leistungsmanagement in IP-Telefonie-Netzwerken.
- Mit eHealth for Voice können Sie Ihre Sprach- und Multimedia-Ressourcen verwalten und gleichzeitig Ihre Risiken und Kosten begrenzen, neue Services bereitstellen und Ihre Investitionen mit den Vorhaben im IT-Bereich abstimmen.

Serviceangebote von CA Technology Services für Netzwerk- und Sprachmanagement

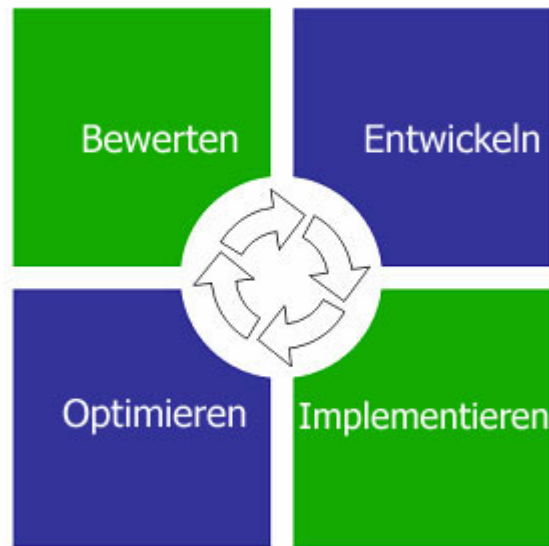
CA Technology Services beschäftigt eHealth- und SPECTRUM-Experten, die Unternehmen bei der Bewertung, Entwicklung, Implementierung und Optimierung von Netzwerk- und Sprachverfügbarkeit und Performance-Lösungen für das gesamte Unternehmen beraten. Unabhängig davon, ob Sie im Finanzdienstleistungssektor, in einem Telekommunikationsunternehmen, einer Regierungsorganisation oder dergleichen tätig sind – die Experten von CA helfen Ihnen dabei, Best Practices-Abläufe einzurichten, Lösungen für das Netzwerkmanagement zu integrieren und die Netzwerk- und Sprachverfügbarkeit sowie die Performance-Lösungen mit dem Service Desk zu kombinieren. Auf diese Weise können Sie das Ereignis-Management-System des Netzwerks konsolidieren.

Die Experten von CA für Netzwerk-/ Sprachverfügbarkeit und Performance stehen Ihnen bei folgenden Zielen zur Seite:

- **Verbesserung der geschäftlichen Ausrichtung**, indem die Netzwerkinfrastruktur auf die kritischen IT-Services abgestimmt und sichergestellt wird, dass sich das Netzwerkteam ausschließlich auf die Bereitstellung der wichtigsten Services des Unternehmens konzentriert.
- **Verbesserung der Planungsfunktionen des Unternehmens**, indem in der gesamten Netzwerkinfrastruktur volle Sichtbarkeit, z. B. in Form von konsolidierten Konsolen, Berichten und Kriterienanalysen, ermöglicht wird.
- **Verringerung von Risiken**, indem automatische Reparaturroutinen definiert und implementiert werden, mit denen die Möglichkeit **menschlicher Fehler** weitgehend verhindert und eine konsistente Problembehandlung gewährleistet wird.
- **Senkung von Kosten**, indem das Netzwerk-Ereignis-Management konsolidiert und in einer zentralen Kontrolleinheit gebündelt wird, um den Bedarf an Personal zu reduzieren.
- **Nutzung des Potenzials der vorhandenen Netzwerkmanagement-Systeme**, indem die aktuell eingesetzten Tools und Arbeitsabläufe integriert und darauf aufbauend neue Prozesse entwickelt werden.
- **Optimierung der Bereitstellung von IT-Services**, indem die Standards von ISO (Internationale Organisation für Normung) und CobiT, die Best Practices von ITIL (IT Infrastructure Library) sowie bewährte Netzwerkmanagementprozesse implementiert werden.

DER LEBENSZYKLUS-ANSATZ VON NETZWERK- UND SPRACHVERFÜGBARKEIT UND PERFORMANCE-LÖSUNGEN

Zwar verfügt jedes Unternehmen über ganz eigene Anforderungen, das Netzwerkmanagement bietet jedoch in Bezug auf die Arbeitsabläufe sowie die Überwachung und Koordination der Managementfunktionen eine Reihe von Anknüpfungspunkten. Die CA-Lösung wird optimiert und an die speziellen Anforderungen Ihres Unternehmens angepasst, indem für den gesamten Lebenszyklus Best Practices und Serviceangebote entwickelt werden.



Bewertung der Situation – Erkennen der Lücken

Zu einer umfassenden Bewertung gehört neben der Einschätzung des aktuellen Stands auch die Einschätzung der Produktivität von Netzwerk- und Sprachverfügbarkeit sowie des Performance-Managements. Die CA-Experten führen eine umfassende Analyse der verschiedenen Bereiche des Netzwerkmanagements durch, wie z. B.:

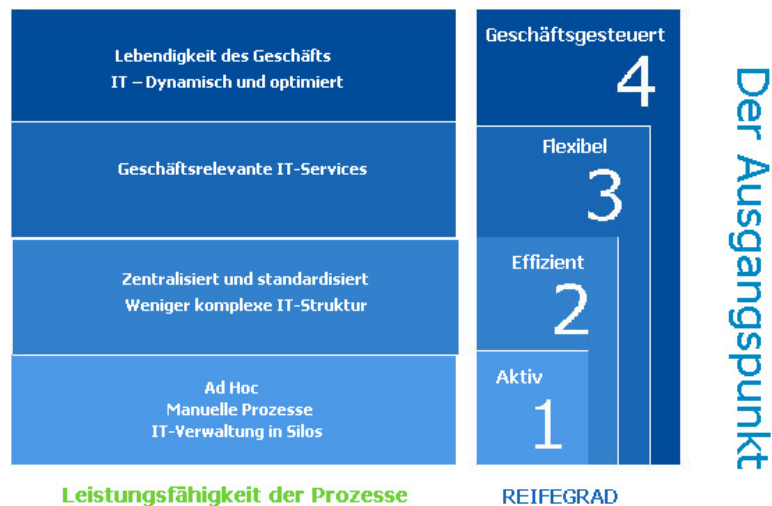
- Vorhaben, Ziele, Funktionen und Strategien des Netzwerkmanagements
- Organisationsstruktur der Netzwerkprozesse, Rollen und Zuständigkeit der Mitarbeiter
- Software zur Überwachung, Konfiguration und Integration des Netzwerks
- Aufbau und Topologie des Netzwerks
- Simulation der Sprachübertragung
- Datenanalyse
- Damit verbundene Sicherheitsanforderungen (Firewalls, Zugriffslisten usw.)
- Definition des Schweregrads von Alarmen/Ereignissen
- Vorhandene betriebswirtschaftliche, technische und ökologische Herausforderungen und Probleme
- Änderung von Steuerungsprozessen
- Anforderungen an die Integration der Produkte von CA und Drittherstellern

Das Ergebnis der aktuellen Managementanalyse wird mit dem CA-Reifemodell für Mitarbeiter, Prozesse und Technologien verglichen, und im Anschluss wird ein entsprechender SAO (Solution Architecture Overview) erstellt. Der SAO ist ein Entwurf, in dem die ausführbaren Lösungsphasen definiert werden, um die Problemerkennung und Reaktionsfähigkeit von Arbeitsabläufen zu maximieren, den Grad der Automatisierung zu erhöhen und Service Desk-Operationen zu integrieren. Die Berater und Architekten von CA analysieren die Netzwerkinfrastruktur, koordinieren diese mit den IT-Services, sprechen Empfehlungen aus und erstellen betriebswirtschaftliche Gutachten zur Sicherung der finanziellen Mittel.

CA-Reifemodelle

Die Best Practices der Branche wurden auf die vier Phasen des IT-Reifemodells abgestimmt. Mit den CA-Reifemodellen werden folgende Ziele verfolgt:

- Ermittlung des aktuellen Stands der IT-Management-Prozesse.
- Bewertung der Reife der IT-Funktionen.
- Ermittlung der schwächsten Prozesse sowie des ROI, der durch die Optimierung und Automatisierung dieser Prozesse erzielt werden kann.



Entwurf – Entwicklung der geeigneten Lösung

Die Architekten von CA entwickeln leistungsfähige Netzwerk-, Sprachverfügbarkeits- und Performance-Lösungen für Unternehmen mit variabler Größe, angefangen bei Einzelstandorten bis hin zu globalen IT-Umgebungen, die rund um die Uhr verfügbar sein müssen und eine entsprechende Hochgeschwindigkeitsleistung benötigen. Der Wertzuwachs wird dadurch erzielt, dass der Service Desk mit den Netzwerken integriert wird, die zur Unterstützung von Anwendungen, Datenbanken, Systemen, Speichermedien und der Sicherheit eingesetzt werden.

Die Architekten setzen sich mit den Kunden zusammen, um die Einschätzungen zu überprüfen oder den aktuellen Stand der Umgebung zu dokumentieren; sie führen Gespräche, um sicherzustellen, dass neben den Zielen des IT-Managements auch die geschäftlichen Interessen gewahrt werden; sie stimmen die Features und Funktionen von eHealth und SPECTRUM auf das Unternehmen und die IT-Anforderungen ab und identifizieren die Hard- und Softwareanforderungen. Im Zuge dieses Prozesses entwirft der Architekt einen umfassenden Entwicklungs- und Implementierungsplan, der auch als SAS (Solution Architecture Specification) bezeichnet wird.

Nur zertifizierte CA-Architekten sind berechtigt, solche Pläne zu entwickeln. Die Qualifizierung zum Architekten erfolgt in einem zweijährigen Intensivprogramm, für das mehrere Branchenzertifizierungen, Schulungen in IT-Management-Technik und CA-Produkten sowie eine vom entsprechenden Gremium erteilte Zulassung als CA-Architekt erforderlich sind. Unsere Architekten müssen sich alle zwei Jahre neu zertifizieren lassen.

Auch Kunden, die eigene Architekten beschäftigen und ihre Entwicklungen intern planen, sind gelegentlich auf Unterstützung angewiesen. Für diese Kunden wird das Solution Expert-Paket von Enterprise Systems Management angeboten, das benutzerdefinierte Richtlinien für kurzfristige Planungen und Prüfungen im Rahmen eines speziell definierten Umfangs enthält.

Implementierung – Die Basis für den Erfolg der Lösung

Die CA-Berater richten auf Basis der SAS die Umgebung ein; sie installieren, konfigurieren und passen Ihre eHealth- und SPECTRUM-Lösungen an; sie überprüfen und dokumentieren die eHealth- und SPECTRUM-Lösungen auf Test-, Qualitätssicherungs- und Produktionssystemen und vermitteln Ihrem Personal die notwendigen Kenntnisse. Im Rahmen dieser Implementierungsservices werden auch Integrationskomponenten zwischen eHealth und SPECTRUM, den anderen IT-Management-Anwendungen und dem Service Desk entwickelt und bereitgestellt.

Damit die einzelnen Implementierungsschritte effektiv koordiniert werden können, werden alle Fortschritte, Fragen, Probleme und Meilensteine von PMP-zertifizierten Projektmanagern verfolgt und protokolliert. CA Technology Services beschäftigt sowohl PMP-zertifizierte Projektmanager als auch hochqualifizierte Architekten, Berater und Partner. Auf das Jahr gerechnet, liegen die Ausgaben, die CA Technology Services in die Weiterbildung seiner Mitarbeiter investiert, 50 % über dem Branchendurchschnitt.

Optimierung – Den Zeitpunkt für Änderungen erkennen

In der Optimierungsphase wird überprüft, inwiefern die vorhandenen eHealth- und SPECTRUM-Lösungen weiter ausgelastet und angepasst werden können. Zum Serviceumfang der eHealth-Prüfung gehören die Anpassung, Neukonfiguration, Aktualisierung und Migration. Darüber hinaus werden Schulungen und Zertifizierungen angeboten, um die Produktivität der Mitarbeiter zu steigern. Die Erfahrungen der Vergangenheit haben gezeigt, dass sich Arbeitsabläufe durch die gezielte Schulung des Personals effizienter gestalten lassen. Die genannten Services werden in zahlreichen Varianten angeboten: vor Ort und außerhalb, mit und ohne Schulungsleiter sowie über das Internet. Schulungsleiter und Kursentwickler sind ebenfalls zertifizierte Experten, die auf Fragen der Netzwerk- und Sprachverfügbarkeit sowie der Performance spezialisiert sind.

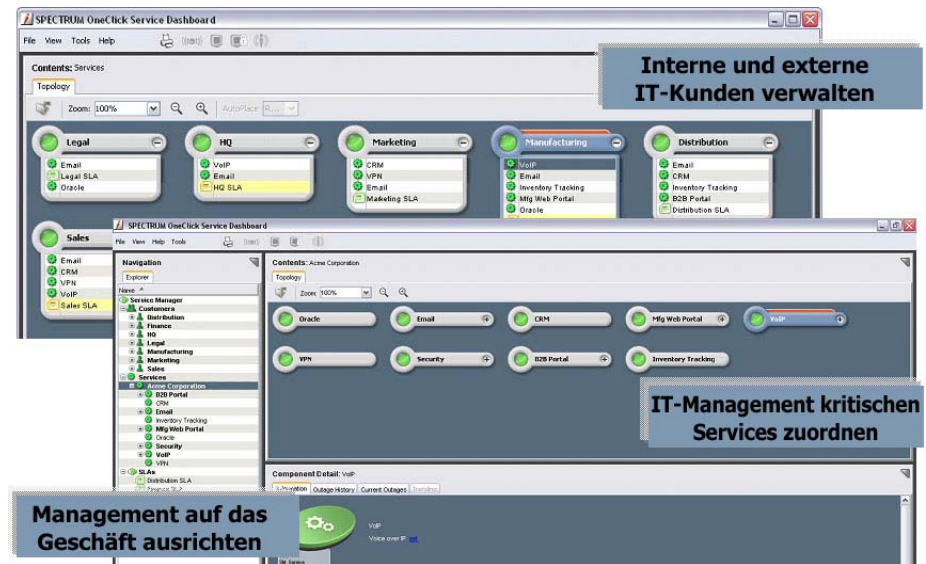
Warum Sie die Verfügbarkeit Ihrer Services CA Technology Services anvertrauen sollten

- **Erfahrung:** CA verfügt über eine mehr als 30-jährige Erfahrung in der Entwicklung von Services für das Enterprise Systems Management.
- **Bewährte Verfahrensweise:** Ein spezialisiertes Bewertungsteam plant, entwirft und erstellt betriebswirtschaftliche Gutachten, die als Empfehlungen für das Netzwerk und die Arbeitsabläufe dienen, und integriert die Best Practices in die Entwürfe des Kunden.
- **Fachliche Kompetenz:** Eine dynamische Gemeinde weltweit agierender Fachleute, die auf Netzwerk- und Sprachverfügbarkeit sowie Performance-Lösungen spezialisiert ist, bringt die in Lösungen gewonnenen Erfahrungen ein und entwickelt kontinuierlich neue Best Practice-Abläufe und Lösungsmodelle.
- **Fokus:** CA Technology Services beschäftigt ein Team von Solution Managern und spezialisierten Architekten, die gezielt an den Bewertungs-, Planungs-, Bereitstellungs- und Arbeitsmethoden arbeiten, die im Rahmen von eHealth- und SPECTRUM-Services und -Lösungen angeboten werden.

Wie die wichtigsten Leistungsmerkmale in der Lösung realisiert sind

Effektives Service-Level-Management

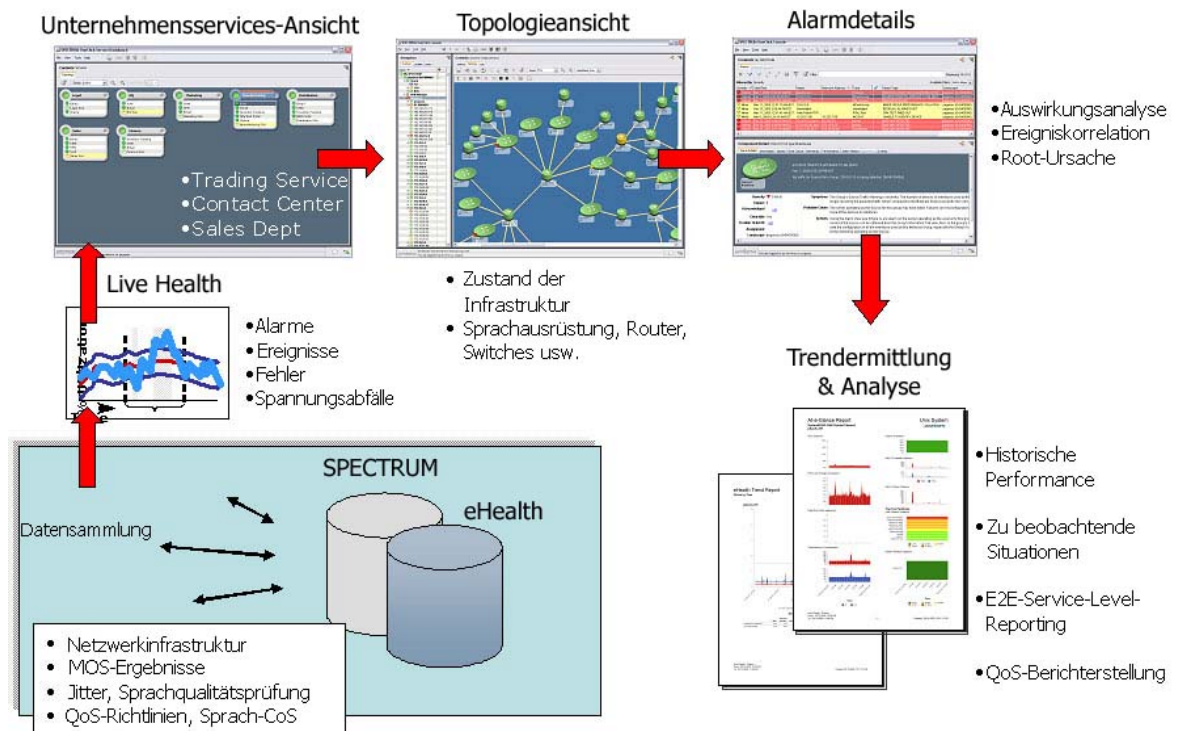
Der SPECTRUM Service Manager zeigt den Status der geschäftskritischen Services an, und zwar in einer Weise, die sowohl für Netzwerkbetreiber als auch für nicht-technisches Personal wie geschäfts- und branchenorientierte Mitarbeiter verständlich ist. Die Informationen zum Status der Services können auf verschiedene Weise angeordnet werden: nach Service, Abteilung (für interne Kunden) oder Kunden (für das Service-Level-Management bzw. die Kommunikation mit externen Kunden).



Proaktive Servicesicherung

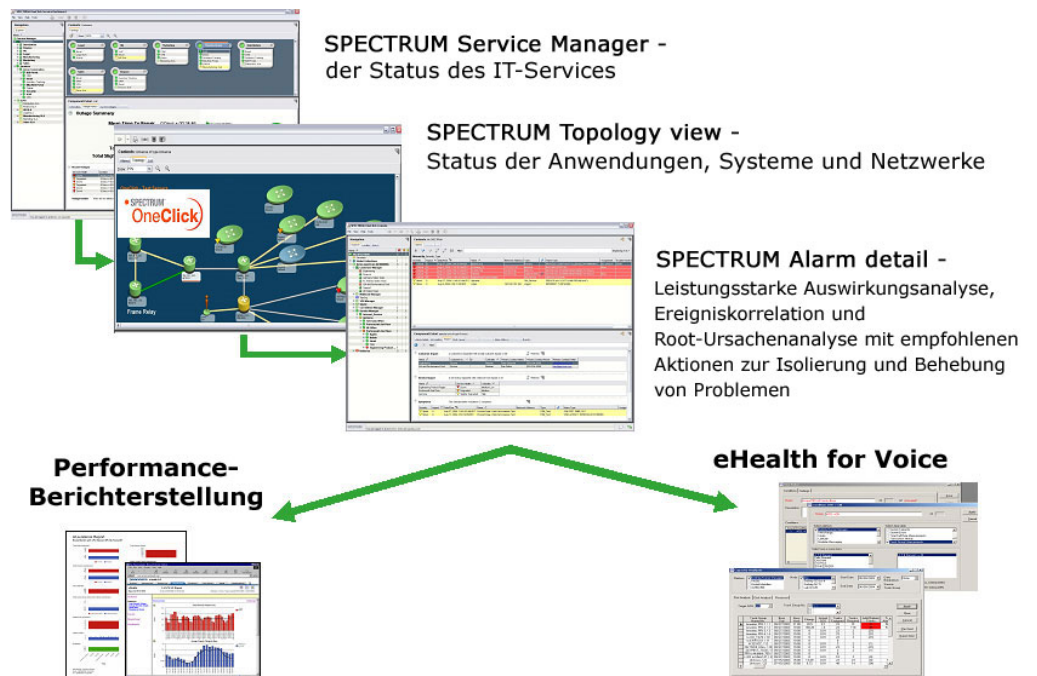
Durch entsprechende Algorithmen, die in allen Produktlinien von CA integriert sind, tragen Netzwerk- und Sprachmanagement-Produkte gemeinsam zur proaktiven Servicesicherung bei. Infolgedessen können die Betreibertteams potenzielle Probleme bereits erkennen, BEVOR sich diese auf die Services für Kunden auswirken.

In eHealth wird dies vorwiegend durch die Algorithmen „Zeitliche Überschreitung von Schwellenwerten“ und „Abweichung von der Norm“ von Live Health erreicht. Sobald die aktuelle Performance einen festgelegten Schwellenwert verletzt oder für eine bestimmte Dauer innerhalb des angegebenen Analysefensters vom Normalverhalten (entsprechend vergangener Erfahrungen) abweicht, wird ein intelligenter, Performance-abhängiger Alert ausgelöst. eHealth for Voice funktioniert auf ähnliche Weise und sendet Alerts, wenn die Größen QoS oder GoS verletzt werden. Die Alerts werden an SPECTRUM weitergeleitet, das anhand der Informationen zu Richtlinien, Modellen und Regeln den Schweregrad des Problems ermittelt und die Alarme entsprechend integriert und korreliert. Dazu werden die SPECTRUM-Funktionen für Service-Management und Sprachmodellierung eingesetzt.



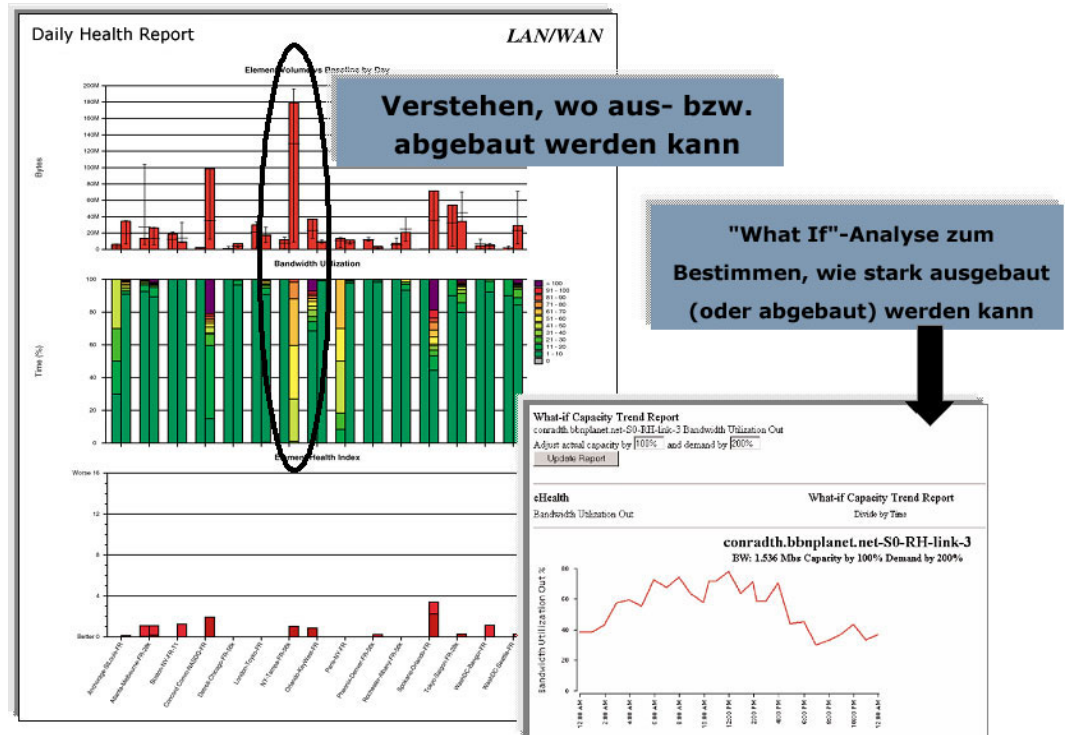
Schnelle Lösung von Problemen

Durch den kombinierten Einsatz von Netzwerk- und Sprachmanagementprodukten können die Netzwerkteams alle Probleme, die im Zusammenhang mit den Sprach- und Dateninfrastrukturen auftreten, umgehend identifizieren und lösen. Im Falle eines Problems werden die Verwaltungsteams zunächst vom SPECTRUM Service Manager benachrichtigt. Der Service Manager zeigt die geschäftskritischen Services an, die je nach den in SPECTRUM definierten Richtlinien mit verschiedenen Farben gekennzeichnet sind. Auf diese Weise können die Mitarbeiter der Verwaltungsteams die für die Infrastruktur problematischen Einheiten in der topologischen Übersicht schnell identifizieren und im Alarmdetailbericht die Details der Alarme (die von eHealth oder von eHealth for Voice gesendet wurden) anzeigen, um das jeweilige Problem besser zu verstehen. Darüber hinaus können sie in SPECTRUM Informationen zu den wahrscheinlichen Ursachen abrufen und anschließend eHealth oder eHealth for Voice starten, um weitere historische Performance-Daten anzuzeigen und die Probleme zu ermitteln, die vor dem aktuellen Problem in der Komponente aufgetreten sind.



Vorausschauende Kapazitätsplanung

Die Netzwerkteams setzen innerhalb von eHealth und eHealth for Voice intelligente Algorithmen ein, um zu ermitteln, wann und wo zusätzliche Kapazitäten erforderlich sind, damit die Zielsetzungen für QoS und GoS erfüllt werden. Auf ähnliche Weise kann auch das umgekehrte Problem gelöst werden, indem die Bereiche identifiziert werden, in denen durch Senkung von Kapazitäten Kosten eingespart werden können, ohne dass sich dies nachteilig auf das Unternehmen auswirkt.



Capacity Analyzer

Platform: ☒ Delinly/Conn Manager ☐ Intuity ☐ Nortel Meridian ☐ OC20-350

Node: ☒ ALL ☐ Delinly G3 LA-4 ☐ Delinly NY-5 ☐ Lab 63.20

Start Date: 05/09/2003 End Date: 05/09/2004

Date Breakdown: None Source: Trunk Group

Post Analysis | Disk Analysis | Processor

Target GOS: 0.1 Trunk Group No.: 1

Apply | Clear | Cancel | Export Grid

Trunk Group Name/No	Buy Day	Buy Hour	Estangs	Actual GOS	Trunks Equipped	Trunks Required	Add/(Delete) Trunks	T1 Alt
Ameltec PRI-1 / 1	09/27/2003	21:00	20.5	0.1	23	21	2	41
Ameltec PRI-2 / 2	09/27/2003	19:00	100.28	> 6	23	118	95	5
Ameltec PRI-3 / 3	09/27/2003	19:00	0	0.01	23	2	21	2
Ameltec PRI-4 / 4	09/27/2003	19:00	0	0.01	23	2	21	2
to HIO_T674 / 10	09/27/2003	19:00	0	0.01	23	2	21	2
to ENR_DS1 / 11	09/27/2003	19:00	0	0	0	0	0	0
H_323ICC / 12	09/27/2003	19:00	0	0.01	3	2	1	1
OUTSIDE CALL / 20	09/27/2003	19:00	0	0.01	23	2	21	2
323-PB2 / 1630 / 3	09/27/2003	19:00	0	0.01	3	2	1	1
PRI to Multlink 780 / 3	09/27/2003	19:00	0	0	0	0	0	0
H_323 to Multlink 147 / 31	09/27/2003	19:00	0	0.01	10	2	8	1
Unknown / 22	07/15/2003	15:00	13.85	0.01	23	23	0	0
Unknown / 23	07/15/2003	15:00	6.72	0.01	48	14	34	1

Eine Kapazitätsanalyse stellt sicher, dass der Ressourcenaufwand optimal ist

(Diese Seite wurde absichtlich leer gelassen)

Kapitel 4:

Implementierungsarchitektur für das Netzwerk- und Sprachmanagement

In diesem Kapitel werden einige einführende Informationen zur Installation und Konfiguration der CA-Lösung für das Netzwerk- und Sprachmanagement gegeben. Dazu werden folgende Hauptthemen behandelt:

- Komponenten der Netzwerkleistung
- Komponenten des Netzwerkfehler-Managements
- Komponenten des Sprachmanagements
- Implementierungsarchitekturen
- Anpassungsempfehlungen

Komponenten der Netzwerkleistung

eHealth besteht aus den folgenden Komponenten:

Erforderliche Komponenten	Optionale Komponenten
E2E Console	Live Health
	Integrationsmodule
	Distributed eHealth
	Remote Poller
	Report Center
	Traffic Accountant

E2E Console

E2E Console bildet das Kernstück der eHealth-Implementierung und wird zur Ausführung von eHealth benötigt. E2E Console stellt neben Datenbank-, Erkennungs- und Pollerfunktionen auch GUIs zur Verwaltung und Berichterstellung sowie weitere Funktionen bereit. Die eHealth-Lizenzen (universelle und systembezogene) ermöglichen es der eHealth-Konsole, mit Hilfe des eingebetteten Management-Software-Agenten Daten von zertifizierten Geräten abzurufen und zu sammeln. Diese Lizenzen werden auch zur Ausführung von eHealth benötigt. Ein Element entspricht dem eHealth-Modell bzw. der Softwaredarstellung einer Infrastrukturkomponente, die mit eHealth analysiert werden kann. eHealth kann zur Analyse physischer Elemente, z. B. eines bestimmten Anschlusses auf einer Karte oder eines Routers, eingesetzt werden. Damit können auch logische Elemente analysiert werden, d. h. Elemente, die auf die logische Funktion eines Geräts oder einer Komponente Bezug nehmen, z. B. eine Netzwerkverknüpfung. Informationen, ob eine Komponente für die gemeinsame Verwendung mit eHealth zertifiziert ist, erhalten Sie auf den Zertifizierungsseiten unter <http://support.concord.com>.

Hinweis: Für den Zugriff auf <http://support.concord.com> benötigen Sie ein Support-Konto. Dieses Konto wird beim Erwerb von eHealth- und SPECTRUM-Produkten eingerichtet.

Live Health

Live Health ist ein Modul zur Überwachung der Echtzeit-Performance, das die von eHealth erhobenen Performance-Daten auf Normabweichungen und die Verletzung von Schwellenwerten überprüft. Live Health besteht aus drei Komponenten:

- Live Exceptions bietet Ihnen die Möglichkeit, in Abhängigkeit von der Performance Alarmer zu definieren und auszulösen.
- Mit Live Status können Sie in einer einzigen durchgängigen Ansicht den Status der gesamten Infrastruktur anzeigen.
- Live Trend stellt Funktionen zum Erstellen von Echtzeit-Berichten bereit.

Integrationsmodule

eHealth bietet eine Reihe von Integrationsmodulen (IMs), die es Ihnen ermöglichen, in eHealth Berichte von den Daten zu erstellen, die von verschiedenen Netzwerkmanagement-Systemen (NMSs) abgerufen werden. Beim Lizenzieren und Installieren eines IM können Sie mit diesem IM Daten aufrufen, die bereits mit einem vorhandenen NMS erfasst wurden. Sie können das IM dann in seiner Gesamtheit in eHealth importieren, um kritische Daten schnell bereitzustellen und um die erforderliche Erfassung redundanter Daten über die Abfrage doppelter Daten zu vermeiden.

- **Universal Workflow IMs** ermöglichen Kunden, von unterstützten Fehlermanagement-Systemen wieder zu eHealth wechseln. Dieser IM-Typ wird auf folgenden Systemen unterstützt: SPECTRUM, IBM (Micromuse) Netcool, Cisco Information Center (CIC) und HP OpenView Network Node Manager.
- **Universal Data IMs** ermöglichen den Import von Konfigurations- und Performance-Daten. Dieser IM-Typ wird auf den folgenden Systemen unterstützt: Cisco WAN Manager, Cisco ISC, Lucent, Alcatel und Nortel.

- **Universal Wireless Data IMs** ermöglichen den Import von Konfigurations- und Performance-Daten von anderen drahtlosen Elementmanagement-Systemen in eHealth E2E Console. Dieser IM-Typ wird auf den folgenden Systemen unterstützt: Nortel Shasta SCS GGSN und Starent ST-16 Bulk Stats.

Distributed eHealth

Bei einer großen Infrastruktur können Sie mehrere Distributed eHealth-Systeme auf verschiedenen physischen Standorten bereitstellen oder anderenfalls gemeinsam in einer zentralen Konfiguration installieren, die als Cluster bezeichnet wird. Der Cluster enthält mehrere eHealth-Systeme, mit denen spezifische Ressourcengruppen verwaltet und die Daten gemeinsam verwendet werden. Durch Verwendung von Distributed eHealth können Sie die Erfassung und Verarbeitung von Daten auf mehrere eHealth-Systeme verteilen, die parallel ausgeführt werden. Berichtsbenutzer können Berichte mit allen Elementen oder Gruppen im Cluster über die Distributed eHealth-Konsolen aufrufen, die für das Cluster als „meldende“ Front-Ends dienen.

In der Regel wählen Sie eine Distributed eHealth-Site, wenn Sie Berichte für eine größere Anzahl Elemente ausführen möchten, die auf einem eigenständigen eHealth-System nicht mehr unterstützt werden kann. Sie können auch eine Distributed eHealth-Site wählen, wenn Sie ein eHealth-Webserverssystem außerhalb der Firewall konfigurieren und die Distributed eHealth-Systeme innerhalb der Firewall der Infrastruktur isolieren möchten. Je nach Anzahl der verfügbaren Distributed eHealth-Systeme und der Systemleistung der Distributed eHealth-Konsole kann eine Distributed eHealth-Site Berichte für bis zu eine Million Elemente unterstützen.

Das Distributed eHealth-Softwarepaket enthält die gesamte Software für Distributed eHealth-Konsolen sowie die erforderliche Software zum Ändern eines eigenständigen eHealth-Systems in ein Distributed eHealth-System. Die Software für die Konsolen, die Elemente und Agenten für die eigenständigen eHealth-Systeme müssen gesondert erworben werden. Umfassende Anweisungen zur Verwaltung eines Clusters finden Sie im *Distributed eHealth Administration Guide*.

Remote Poller

Bei einer großen oder weitreichenden Umgebung können mit einem eHealth-System möglicherweise nicht alle Ressourcen überwacht werden. Mit Hilfe von Remote Polling können Sie eHealth auf Remotesystemen (als Remotesites bezeichnet) installieren und die einzelnen Sites so konfigurieren, dass jeweils eine Gruppe von Elementen abgefragt wird. Die Datenbank auf jeder eHealth-Remotesite enthält die Daten für die Elemente, die sie abfragt. Über eHealth auf den einzelnen Sites können Sie diese Elemente verwalten. Mit einem zentralen eHealth-System werden die Elementdaten und Performance-Daten dann in regelmäßigen Abständen von den eHealth-Remotesystemen abgerufen und in einer zentralen eHealth-Datenbank zusammengeführt. Über diese zentrale Datenbank können Sie Berichte für alle Elemente ausführen.

Im Allgemeinen wählen Sie eine Remote Polling-Site, wenn es wichtig ist, dass die Abfragesysteme unabhängig voneinander sind und Daten nicht gemeinsam verwendet werden. Über die Remotesites können beispielsweise jeweils unterschiedliche Kunden eines Serviceanbieters oder einzelne Unternehmensbereiche einer großen Organisation verwaltet werden. Bei Remote Poller-Sites kann es sich um räumlich getrennte Standorte oder um lokale Sites handeln, die durch Firewalls oder andere Barrieren getrennt sind, aufgrund derer sich Abfragen verzögern oder nicht möglich sind. Umfassende Anweisungen zur Verwaltung eines Remote Poller-Systems finden Sie im *Using the eHealth Remote Poller Guide*.

Report Center

eHealth Report Center ist eine optionale Anwendung zur Berichterstellung, die mit eHealth ab Version 6.0 zur Verfügung gestellt wird. Diese Anwendung stellt eine Alternative zu eHealth Report Developer Language (RDL) dar, mit der eHealth-Standardberichte angepasst werden können. Mit Hilfe von Report Center können Benutzer gänzlich neue eHealth-Berichtstypen erstellen und individuell anpassen. Mit diesen Berichten können verschiedene Belange zur Leistung des Netzwerks, des Systems und der Anwendungsressourcen abgedeckt werden.

Report Center bietet hohe Flexibilität und große Anpassungsmöglichkeiten und verfügt über umfassende Funktionen, mit denen Benutzer die Darstellung von Berichten und vorhandenen eHealth-Daten bearbeiten können. Die Anwendung umfasst eine webbasierte Benutzeroberfläche mit einer Windows-ähnlichen Verzeichnisstruktur, die Benutzer nach ihren Anforderungen ändern können. Über diese intuitive Benutzeroberfläche ist es einfach, Berichte schnell zu identifizieren, anzuzeigen und auszuführen. Report Center enthält nützliche Beispielberichte, die Benutzer ausführen können, um die Performance der Ressourcen anzuzeigen, oder beim Erstellen neuer Berichte als Vorlagen verwenden können.

Traffic Accountant

Die meisten Unternehmen mit Internet- und E-Business-Strategien müssen gewährleisten, dass ihre Netzwerkressourcen optimal an die Bedürfnisse der Benutzer sowie an die Anforderungen der Anwendungen angepasst sind. Die Kenntnis der Bandbreitennutzer und der verwendeten Anwendungen ist von großer Bedeutung. Mit Traffic Accountant können Sie den Netzwerkdatenverkehr mit dem Industriestandard entsprechenden RMON2-Probes sowie mit NetFlow-fähigen Cisco-Routern überwachen. Traffic Accountant umfasst komplexe Gruppierungs- und Sortierungsfunktionen zum Erstellen präziser und leicht zu verstehender Berichte. So erhalten Sie Einblicke in Trends und Verwendungsmuster, die sich auf die Performance des Netzwerks auswirken. Traffic Accountant erfordert ein dediziertes eHealth-System: Wenn Sie den RMON2-Datenverkehr sowie den Standard-NetzwerkLeistungsverkehr überwachen möchten, benötigen Sie zwei eHealth-Systeme, um sicherzustellen, dass eine optimale Abfrage- und Berichterstellungsleistung erzielt wird.

Komponenten des Netzwerkfehler-Managements

SPECTRUM umfasst die folgenden Komponenten:

Erforderliche Komponenten	Optionale Komponenten	
Assurance Server	Watch Editor	ATM Circuit Manager
Assurance Server Xsight	SNMP V3	Report Manager
Assurance Server Integrity	Alarm Notification Manager	Multicast Manager
Assurance Server Infinity	Secure Domain Manager	Service Performance Manager
OneClick	Frame Relay Manager	QoS Manager
	Configuration Manager	Service Manager
	VPN Manager	

Assurance Server

SPECTRUM verfügt über drei verschiedene Assurance Server-Komponenten für unterschiedliche Kundentypen:

- Assurance Server Xsight (für junge Unternehmen)
- Assurance Server Integrity (für größere Unternehmen)
- Assurance Server Infinity (für Serviceanbieter)

ASSURANCE SERVER XSIGHT

Mit Assurance Server Xsight werden die Funktionen der SPECTRUM-Hauptverfahren einer größeren Anzahl kleinerer Unternehmen zur Verfügung gestellt. Mit SPECTRUM Xsight hat CA eine Paketlösung für das IP-Fehler- und Leistungsmanagement eingeführt, das zu einem attraktiven Preis angeboten wird und einen schnellen Einstieg ermöglicht. Diese Komponente unterstützt die Geräte der meisten Hersteller, die heutzutage in Unternehmensnetzwerken eingesetzt werden. Dabei beschränkt sich die Unterstützung jedoch auf die Implementation auf einem Server; eine verteilte Implementation wird nicht unterstützt.

Assurance Server Xsight umfasst die folgenden wichtigen Funktionen:

- Ursachenanalyse
- Auswirkungsanalyse
- Auto-Discovery von Netzwerken mehrerer Hersteller und Technologien
- Standardbasierte Integrationen
- Eine gemeinsame Administratorlizenz (Fehlertoleranzlizenz nicht inbegriffen)

ASSURANCE SERVER INTEGRITY

SPECTRUM ist in erster Linie für große Unternehmen mit häufig auftretenden Änderungen, Zusammenführungen und Skalierungen ausgelegt. Mit der SPECTRUM Integrity-Lösung werden die patentierten CA-Technologien transformiert und mit neuen Funktionen kombiniert, um den heutigen sich entwickelnden Unternehmen Möglichkeiten bereitzustellen, geschäftsentscheidende Services innerhalb des Unternehmens oder weltweit zu verwalten. Diese Komponente unterstützt die Geräte der meisten Hersteller, die heutzutage in Unternehmensnetzwerken eingesetzt werden.

Assurance Server Integrity umfasst die folgenden wichtigen Funktionen:

- Ursachenanalyse
- Auswirkungsanalyse
- Auto-Discovery von Netzwerken mehrerer Hersteller und Technologien
- Standardbasierte Integrationen
- Eine Administratorlizenz und eine Fehlertoleranzlizenz

ASSURANCE SERVER INFINITY

SPECTRUM Infinity konzentriert sich speziell auf die Anforderungen heutiger Serviceanbieter. Die Komponente enthält spezifische Funktionen mit erheblichen Leistungsverbesserungen, um die Markteinführung neuer Services zu beschleunigen sowie die Qualitätserwartungen der Kunden zu übertreffen, und bietet gleichzeitig die Möglichkeit, eine wachsende Infrastruktur mit vorhandenen Ressourcen zu verwalten. Diese Komponente umfasst Integrity-Geräteunterstützung und das Advanced Management Module, das die hochwertigen Geräte unterstützt, die normalerweise nur in Netzwerken von Serviceanbietern eingesetzt werden.

Assurance Server Infinity umfasst die folgenden wichtigen Funktionen:

- Ursachenanalyse
- Auswirkungsanalyse
- Auto-Discovery von Netzwerken mehrerer Hersteller und Technologien
- Standardbasierte Integrationen
- Eine Administratorlizenz, eine Fehlertoleranzlizenz und zwei Lizenzen für die Southbound Gateway-Integration

OneClick

SPECTRUM OneClick ist eine dreischichtige, webbasierte Konsole. Die zentrale Komponente ist ein Webserver, der direkt mit SPECTRUM Assurance Servers verbunden wird und Daten für verteilte Java-Clients bereitstellt. Die funktionsreichen Java-Clients werden über den OneClick-Webserver heruntergeladen, installiert und aktualisiert, um die Implementierung, Verwaltung und Wartung zu vereinfachen. Die SPECTRUM OneClick-Konsole kombiniert den Zugriff ohne örtliche und zeitliche Beschränkung mit der Skalierbarkeit und Schnelligkeit einer vollständigen Desktop-Clientanwendung und reduziert so die Schulungsanforderungen von herkömmlichen webbasierten Anwendungen.

Die OneClick-Konsole umfasst die folgenden wichtigen Funktionen:

- Ereigniskonsole
- Rollenbasierte, intuitive Weboberfläche
- Umfassende Topologiestrukturen
- Hoch konfigurierbare Alarmkonsole
- Vollständige Suite mit Tools zur Problembehandlung
- Managementsicherheit
- Automatisierte Client-Installation
- Lizenzierung für parallele Verwendung

Watch Editor

SPECTRUM Watch Editor stellt eine einfache Möglichkeit zur Überwachung wichtiger Leistungsindikatoren in Netzwerk-, System- und Anwendungsinfrastrukturen dar. Mit Hilfe von Watch Editor kann die Überwachung angepasst und erweitert werden. Durch Hinzufügen zusätzlicher Funktionen für Abfrage, Anmeldung und Schwellenwertüberwachung zu SPECTRUM können Benachrichtigungen automatisiert und Skripts gestartet werden, wenn sich die Leistung ändert oder außerhalb der normalen Baselines liegt.

Mit Überwachungen können statistische Angaben, komplexe Berechnungen und/oder Werte kontrolliert werden, die statisch bleiben sollen. Überwachungen können zudem parallel für Tausende von Geräten konfiguriert und angewendet werden. Kunden überwachen mit SPECTRUM Watch Editor häufig Prozessor-, Speicher- und Bandbreitennutzung von Geräten verschiedener Hersteller und Technologien. Durch die Zusammenwirkung dieser Funktionen wird eine kosteneffiziente Möglichkeit zur intelligenten Schwellenwertüberwachung mit proaktiven automatisierten Korrekturmaßnahmen ohne komplexe Programmierungsverfahren angeboten.

Watch Editor umfasst die folgenden wichtigen Funktionen:

- Einfaches Erstellen proaktiver Schwellenwerte für wichtige Leistungsindikatoren für Netzwerk-, System- und Anwendungsinfrastrukturen
- Automatisieren von Korrekturmaßnahmen
- Aktivieren von Überwachungen anhand von Timern, Abfragen, statistischen Angaben und berechneten Werten

Alarm Notification Manager

Mit SPECTRUM Alarm Notification Manager (SANM) wird der Funktionsumfang von SPECTRUM zur Alarmverarbeitung erweitert. Mit Hilfe von SANM Policy Administrator können Sie die gewünschten Alarmtypen festlegen und die als unwichtig eingestuft Alarme herausfiltern. Über die SANM-Benutzeroberfläche mit Zeigen-und-Klicken-Funktionalität kann das Alarmverhalten zudem anhand von Parametern zur stündlichen, täglichen, wöchentlichen oder monatlichen Planung gesteuert werden. Große Unternehmen und Serviceanbieter setzen SANM routinemäßig für Netzbetriebszentren ein, die remote von einem Administrator verwaltet werden. Bestimmte IT-Mitarbeiter können entsprechend ihrer Arbeitszeit und unabhängig von ihrem Aufenthaltsort mit Hilfe von SPECTRUM über Probleme benachrichtigt werden und haben so Ursachendaten vorliegen. Über SANM werden unternehmensbezogene Alarme in der Unternehmenssprache an Führungskräfte übermittelt, während technische Alarme in technischer Sprache an IT-Mitarbeiter gesendet werden. Mit dieser Komponente können Sie für Ihre SPECTRUM-Umgebung kosteneffizient Richtlinien für Alarmbenachrichtigungen verwalten.

Alarm Notification Manager umfasst die folgenden wichtigen Funktionen:

- Alarmkonsolidierung
- Alarmfilterung
- Richtlinienbasierte Alarmweiterleitung
- Alarmbenachrichtigung

Frame Relay Manager

SPECTRUM Frame Relay Manager gibt präzise Überwachungs- und Leistungsschwellenwerte für CIR (Committed Information Rates), Bandbreitennutzung und Verbindungsstau aus. Ursachen- und Fehleranalyse werden mit Auswirkungsanalyse über DLCI (Data Link Connection Identifier) bereitgestellt, um Antwort und Korrekturmaßnahmen zu priorisieren. Patentierte intelligente Auto-Discovery-Verfahren ordnen die DLCI-Konnektivität unter Ausnutzung von Remote-IP-Adressinformationen und Datenübertragungsstatistiken entsprechend zu und erzeugen eine integrierte Topologieansicht. Etliche große Unternehmen dokumentieren mit Hilfe von SPECTRUM Frame Relay Manager SLA-Verstöße durch ihre Serviceanbieter.

Mit SPECTRUM Frame Relay Manager kann darüber hinaus ermittelt werden, ob ein Unternehmen pro Verbindung zu viel oder zu wenig Bandbreite erworben hat. Dies kann zu Kosteneinsparungen von mehreren Tausend Euro pro Monat bei WAN-Verbindungskosten führen. Serviceanbieter haben SPECTRUM Frame Relay Manager eingesetzt, um die SLA-Einhaltung sicherzustellen, die Qualität des Kundenservices zu verbessern sowie differenzierte Serviceangebote bereitzustellen. Durch Verwendung dieser Komponente kann ein Serviceanbieter Frame-Relay-Probleme in 97 bis 99 % der Fälle vor seinen Kunden ermitteln und beheben, bevor diese sich auf die Kundenunternehmen auswirken. Mit Hilfe dieser Komponente wird eine kosteneffiziente Möglichkeit bereitgestellt, die Servicequalität zu verbessern, eine durchgängige Sichtbarkeit zu erzielen und Betriebskosten zu reduzieren.

Frame Relay Manager umfasst die folgenden wichtigen Funktionen:

- Proaktive Kommunikation mit Frame-Relay-Geräten mit Unterstützung von RFC 1315- oder RFC 2115-Frame-Relay-MIBs mit Herstellererweiterungen für Cisco und Nortel
- Schnelle, akkurate Modellierung physischer und logischer DLCI-Anschlusskonnektivität mit IP-Adresse, Subnetz-Maske und Remote-IP-Adressinformationen
- Auflistung von CIR-Durchsatz, Blockierungsstatistiken und DTE-Änderungen (Data Terminal Equipment, Datenendeinrichtung) in vorgegebenen Leistungsansichten

ATM Circuit Manager

SPECTRUM ATM Circuit Manager gibt präzise Überwachungs- und Leistungsschwellenwerte für ATM-Durchsatz, Bandbreitennutzung und Verbindungsstau aus. Ursachen- und Fehleranalyse werden für virtuelle private LANs (VPL)/virtuelle Links auf Kanalebene (VCL) mit einer Auswirkungsanalyse bereitgestellt, um Antwort und Korrekturmaßnahmen zu priorisieren. Patentierte intelligente Auto-Discovery-Verfahren ordnen die VPI-Konnektivität (Virtual Path Identifier) und die VCI-Konnektivität (Virtual Channel Identifier) unter Ausnutzung von Remote-IP-Adressinformationen und Datenübertragungsstatistiken entsprechend zu und erzeugen eine integrierte Topologieansicht. In der Ansicht für den ATM-Circuit-Pfad ist die Endpunktzurordnung für alle durchlaufenen Geräte, physischen Anschlüsse und logischen Schnittstellen aufgeführt.

Unternehmen können zudem eine Liste der permanenten virtuellen Verbindungen (PVCs) importieren, die von ihrem Serviceanbieter bereitgestellt wurden, um alle ATM WAN-Links akkurat zu modellieren. Etliche große Unternehmen dokumentieren mit Hilfe von SPECTRUM ATM Circuit Manager bereits SLA-Verstöße durch ihre Serviceanbieter. Neben dieser Funktion kann mit SPECTRUM ATM Circuit Manager darüber hinaus ermittelt werden, ob ein Unternehmen pro Verbindung zu viel oder zu wenig Bandbreite erworben hat. Dies kann zu Kosteneinsparungen von mehreren Tausend Euro pro Monat bei WAN-Verbindungskosten führen. Serviceanbieter haben SPECTRUM ATM Circuit Manager eingesetzt, um die SLA-Einhaltung sicherzustellen und differenzierte Serviceangebote bereitzustellen. Mit Hilfe dieser Komponente wird eine kosteneffiziente Möglichkeit bereitgestellt, die Servicequalität zu verbessern, eine durchgängige Sichtbarkeit zu erzielen und Betriebskosten zu reduzieren.

ATM Circuit Manager umfasst die folgenden wichtigen Funktionen:

- Proaktive Kommunikation mit ATM-Geräten mit Unterstützung von RFC 1695 mit privaten Management Information Bases (MIBs)
- Schnelle, akkurate Modellierung physischer und logischer VPL/VCL-Anschlusskonnektivität mit IP-Adresse, Subnetz-Maske und Remote-IP-Adressinformationen
- Auflistung des Durchsatzes (Zellen pro Sekunde) und der ATM-QoS-Informationen in vorgegebenen Leistungsansichten

Multicast Manager

SPECTRUM Multicast Manager ermöglicht die Sichtbarkeit von Geräten mehrerer Hersteller in logischen Multicast-Netzwerksitzungen, d. h., die wichtigen Leistungsindikatoren werden proaktiv überwacht, und die Auswirkungen der Infrastrukturausfälle auf Multicast-Services werden hervorgehoben. Alle logischen Multicast-Überlagerungsservices werden automatisch erkannt und innerhalb von SPECTRUM Assurance Server modelliert. Multicast-Sitzungsmodelle umfassen vollständige Angaben zur Multicast-Einspeisung, einschließlich der Quelle, der Verteilungsstruktur und der Empfänger.

SPECTRUM Multicast Manager bietet Benutzern eine leicht bedienbare Oberfläche zur Topologienavigation und Alarmüberwachung. Dies führt zu reduzierten Schulungs- und Verwaltungskosten, da Benutzer Zugriff auf umfassende handlungsrelevante Informationen haben. Durch Multicast-Erweiterungen können Benutzer die Multicast-Topologie pro Gruppe sowie die zugeordneten Router, Switches und Anschlüsse anzeigen, die die IP-Multicast-Gruppe bilden. Mit SPECTRUM Multicast Manager wird zudem der Zustand von Multicast-Gruppen überwacht. Wenn bei einer Ressource in einer Multicast-Gruppe (Quelle, Router, Switches, Anschlüsse) ein Zuverlässigkeitsproblem auftritt, werden mit Hilfe von SPECTRUM Multicast Manager automatisch die Auswirkungen auf die Gesamtgruppe erkannt. Mit dieser Komponente können Sie Ihre Multicast-Infrastruktur kosteneffizient als Unternehmensservice verwalten.

Multicast Manager umfasst die folgenden wichtigen Funktionen:

- Ansicht der IP-Services mehrerer Hersteller mit einer detaillierten Aufgliederung der Elemente, die eine Multicast-Gruppe bilden
- Intuitive Benutzeroberfläche zur Multicast-Topologienavigation und Alarmüberwachung von Gruppen, Quellen, Empfängern und RP-Geräten (Rendezvous Point)

QoS Manager

Mit Hilfe von SPECTRUM QoS Manager können Unternehmen und Serviceanbieter die Konfiguration und Effektivität von QoS-Richtlinien und Übertragungsklassen in der gesamten IP-Infrastruktur überprüfen und validieren. Mit Technology Relationship Mapping und der webbasierten Berichterstellung wird der Zustand und die Performance der einzelnen im Netzwerk konfigurierten CoS-Komponenten erkannt und dokumentiert. Mit patentierten SPECTRUM-Analysen wird die Modellierung der QoS-Richtlinien und Übertragungsklassen intelligent integriert und automatisiert, um Ursachenanalyse und Auswirkungspriorisierung zu gewährleisten.

In SPECTRUM wird eine einheitliche Ansicht der QoS-fähigen Infrastruktur mit einem benutzerfreundlichen Explorer/Navigator angezeigt, über die Sie auf die Daten auf Geräte- und Anschlussebene zugreifen können, die einer Übertragungsklasse zugeordnet sind. Darüber hinaus können Benutzer in SPECTRUM alle konfigurierten Verhalten sowie vollständige statistische Angaben zu Policing, Shaping, Queuing und Random Early Detection (RED) anzeigen. Benutzer haben Zugriff auf handlungsrelevante Alarminformationen, wenn innerhalb einzelner Klassen hohe Raten von Packet Drops oder Buffer Queuing festgestellt werden.

QoS Manager umfasst die folgenden wichtigen Funktionen:

- Navigieren zu und Zugriff auf Daten auf Geräte- und Anschlussebene, die einer bestimmten Übertragungsklasse zugeordnet sind
- Vorgegebene Leistungsansichten für statistische Angaben zur QoS-Übertragung, z. B. Policing, Shaping, Queuing oder RED

VPN Manager

Über SPECTRUM VPN Manager können Unternehmen und Serviceanbieter automatisch die Performance und Zuverlässigkeit von Site-to-Site-Layer-3-VPN-Kanälen erkennen und verwalten. Durch die proaktive Benachrichtigung über potenzielle Probleme wird sichergestellt, dass Korrekturmaßnahmen ergriffen werden, bevor sich Auswirkungen auf kritische Services und Kunden ergeben. Mit Hilfe von SPECTRUM VPN Manager wird die physische und logische Konnektivität dynamisch erkannt und die Verfügbarkeit über VRF-Heartbeat-Überwachung (VRF = Virtual Routing and Forwarding) geprüft. Mit dieser Komponente können Sie in Ihrer VPN-Infrastruktur kosteneffizient eine integrierte Fehler- und Performanceverwaltung einsetzen.

VPN Manager umfasst die folgenden wichtigen Funktionen:

- Logische VPN-Topologie
- Proaktive Kommunikation mit VPN-Geräten mit Unterstützung von RFC 2547 BGP/MPLS VPN-MIB mit Erweiterungen privater Hersteller
- Schnelle, akkurate Modellierung physischer und logischer VPN-Verbindungen
- Vorgegebene Leistungsansichten von individuellem Tunnel und aggregierten VPN-Statistiken

SNMPv3

Mit SPECTRUM SNMPv3 können Sie sichere Managementverbindungen herstellen. Die Lösung umfasst ein Übersetzungsmodul für SNMP v1- und SNMPv3-Anforderungen und -Antworten. Die SNMPv3-Technologie unterstützt die Verbindung mit Netzwerk-, System-, Speicher-, Datenbank-, Anwendungs- und Sicherheitsinfrastrukturkomponenten, die Proxyverwaltung älterer Systeme sowie die Manager-to-Manager-Kommunikation. Kunden können die volle Bandbreite der SNMPv3-Authentifizierung und der Verschlüsselungsfunktionen einsetzen, um eine vollständig sichere Managementdatenübertragung und eine sichere Konfiguration/Steuerung der IT-Infrastrukturkomponenten zu gewährleisten.

SPECTRUM SNMPv3 umfasst die folgenden wichtigen Funktionen:

- Schutz vor Sicherheitsbedrohungen
- Authentifizierung
- Datenschutz
- Bestätigung
- Leistungsstarke Zähler

Secure Domain Manager

Heutzutage sind komplexe und verteilte Netzwerke durch Sicherheitsrichtlinien gekennzeichnet, die die Verwendung nicht sicherer Verwaltungsprotokolle wie Simple Management Network Protocol 1 (SNMP) oder Internet Control Message Protocol (ICMP) zur Verwaltung dieser Netzwerke verhindern. Beispielsweise trennt eine DMZ (Demilitarized Zone, engl. für: Entmilitarisierte Zone) aus Sicherheitsgründen mehrere Elemente durch eine Firewall vom Intranet ab. Dennoch müssen Unternehmen, Prozesse und Kunden weiterhin von IT-Services unterstützt werden. Hierfür ist ein Einblick in die gesamte Infrastruktur erforderlich. SPECTRUM Secure Domain Manager (SDM) ermöglicht Kunden die Verwaltung solcher Domänen durch sicheres Tunneling des SNMP- und ICMP-Verkehrs über eine SSL-(Secure Sockets Layer-)Verbindung. In die Firewall muss nur eine einzige Öffnung eingefügt werden, um erweiterte Verwaltbarkeit ohne Auswirkungen auf die geltenden Sicherheitsrichtlinien zu ermöglichen. Diese Lösung ist für den Endbenutzer und alle Clientanwendungen völlig transparent, so dass keine zusätzlichen administrativen Aufgaben durchgeführt werden müssen.

Hinweis: Diese Funktion ist für Assurance Server Xsight nicht verfügbar.

Secure Domain Manager umfasst die folgenden wichtigen Funktionen:

- Mehrere sichere Domänenkonnektoren
- Weiterleitung von SNMP- und ICMP-Verkehr
- Sicherer Tunnelverkehr mit XML/SSL über TCP (Transmission Control Protocol)
- Transparenz für Benutzer und Clientanwendungen

Configuration Manager

Zum Management der heutigen komplexen Infrastrukturen gehört die Verwaltung von Hunderten oder sogar Tausenden geschäftskritischen Geräten. Es kann äußerst anstrengend sein, ihre Konfigurationen zu verfolgen und sicherzustellen, dass die jeweiligen Konfigurationen korrekt sind. SPECTRUM Configuration Manager ist eine intelligente und integrierte Anwendung, mit der die Verwaltung kritischer Gerätekonfigurationen automatisiert und die Betriebsfähigkeit von Unternehmen sichergestellt werden kann. SPECTRUM Configuration Manager stellt Tools bereit, mit denen Sie Konfigurationen für Tausende Geräte verschiedener Hersteller erfassen, bearbeiten, laden und überprüfen können. Das einzigartige Design von SPECTRUM Configuration Manager ermöglicht Benutzern, die Geräteadministration mit Hilfe von Konfigurationsdateien, MIB-Objektbezeichner (OIDs) und SNMP-Attributen durchzuführen. Jede Konfiguration erhält einen Zeitstempel und wird durch die Revisionsnummer identifiziert. SPECTRUM-spezifische Werte, z. B. Abfrageintervall, Community-Name oder Sicherheitszeichenfolge, können bearbeitet werden.

SPECTRUM Configuration Manager ermöglicht, gespeicherte Konfigurationen auf einzelne oder mehrere Geräte gleichzeitig zu laden und dabei alle Änderungen zu verfolgen, automatisches Hochladen in den Wartungsfenstern zu planen oder Konfigurationen auf ihren letzten korrekten Status zurückzusetzen. Durch automatisch geplante Konfigurationsvergleiche werden Sie sofort über nicht autorisierte Änderungen benachrichtigt. Diese Komponente bietet kosteneffektives Konfigurationsmanagement zur Sicherung der Geschäftskontinuität.

Configuration Manager ermöglicht die folgenden wichtigen Funktionen:

- Erfassung von Konfigurationen
- Bearbeitung von Konfigurationen
- Laden und Wiederherstellen von Konfigurationen
- Vergleich und Validierung von Konfigurationen
- Automatisierte Planung

Report Manager

SPECTRUM Report Manager zeichnet sich durch eine unkomplizierte Installation und Implementation aus und nutzt die von SPECTRUM erfassten Verfügbarkeits-, Leistungs-, Asset- und Qualitätsdaten. Anhand der über das Web oder verschiedene Exportformate bereitgestellten Informationen können Sie Probleme proaktiv identifizieren und Korrekturmaßnahmen einleiten, bevor geschäftskritische Services und Kunden beeinträchtigt werden. SPECTRUM Report Manager ermöglicht Asset- und Verfügbarkeitsanalysen nach Hersteller, Produktreihe und Art des Geräts und trägt so dazu bei, die Investitionsrentabilität zu steigern. Laut Studien ermöglichen die aus Ressourcenbestandsberichten gewonnenen Kenntnisse über die Ressourcenauslastung und -zuordnungsmöglichkeiten, den Investitionsaufwand im ersten Jahr um 30 % zu verringern und 5 bis 10 % der laufenden Betriebskosten einzusparen. Anhand von Verfügbarkeitsberichten kann ermittelt werden, wie sich Hersteller und/oder bestimmte Produkte auf die Servicequalität auswirken, so dass IT-Investitionsentscheidungen auf der Grundlage von Fakten getroffen werden können. Mit SPECTRUM Report Manager kann Ihre Organisation die gesamte Verfügbarkeit, Performance und Servicequalität der End-to-End-IT-Infrastruktur beurteilen.

Report Manager ermöglicht die folgenden wichtigen Funktionen:

- automatisierte Berichtverfassung
- automatisierte Berichtverteilung per E-Mail
- Export in Adobe PDF-, Microsoft Excel- und Word-Format
- Eine gleichzeitige Benutzerlizenz

Service Performance Manager

SPECTRUM Service Performance Manager (SPM) bietet einen Ansatz für das Leistungsmanagement, der viele Hersteller und Agenten berücksichtigt, und ermöglicht die effektive Nutzung der vorhandenen Investitionen für das Antwortzeitmanagement. Durch die intelligente und automatische Discovery und Konfiguration der Performance Test Points in der Infrastruktur wird die Implementation beschleunigt und die Effizienz der Arbeitsabläufe optimiert. Mit den Funktionen für die Fehlerbeseitigung in Echtzeit können IT-Mitarbeiter die Ursache von Leistungsverschlechterungen rasch isolieren sowie nach der Durchführung von Korrekturmaßnahmen die Leistung testen und überprüfen.

Eine langsame Anwendung wird von Endbenutzern als defekte Anwendung wahrgenommen. SPM ermöglicht Kunden durch die effektive Nutzung der bereits in ihrer Infrastruktur bereitgestellten Funktionen zur Antwortzeitmessung, die Performance proaktiv zu messen und Netzwerk-, System- oder Anwendungsprobleme zu erkennen. Nach der Durchführung der Korrekturmaßnahmen kann mit Echtzeittests überprüft werden, ob die Reparaturen erfolgreich waren. SPM bietet eine einfache Methode für die automatische Discovery von Performance-Test-Hosts, Benachrichtigung bei Schwellenwertverletzungen, zentrale Fehlerbehandlung sowie die Erfassung statistischer Leistungsdaten zur Berichtverfassung und für weitergehende Analysen. Dies führt zu besseren Leistungen und erhöht die Zufriedenheit der Benutzer.

Service Performance Manager ermöglicht die folgenden wichtigen Funktionen:

- Echtzeitbenachrichtigung über Schwellenwertverletzungen auf Grundlage geplanter Antwortzeittests
- Baseline- und Schwellenwertanalysen
- automatische Discovery von Response-Time-Agenten
- wirksamer Einsatz der vorhandenen Investitionen durch die vollständige Nutzung der aktuell bereitgestellten Performance-Agenten: Cisco IP SLA (SAA & RTTMON), Cisco Ping MIB, Nortel Ping MIB, RFC 2925 (Extreme, Juniper, Riverstone), SystemEDGE, Micromuse (Network Harmoni SLA+)

Service Manager

SPECTRUM Service Manager nutzt die Business Service Intelligence von SPECTRUM, um Echtzeit- und Verlaufsmanagement für Geschäftsprozesse, SLAs und Kunden zu ermöglichen. Anstatt die Verwaltung in einem bestimmten vertikalen Technologiesilo (Netzwerk, Systeme, Anwendungen usw.) fortzuführen, ermöglicht SPECTRUM Service Manager eine horizontale siloübergreifende Verwaltung, die mit Zuverlässigkeit der Geschäftsprozesse einhergeht.

Dieses Tool kennt die physischen und logischen Beziehungen zwischen Verfügbarkeit und Performance der IT-Infrastrukturkomponenten und den wichtigen Services und Kunden, die sie unterstützen sollen. Zugehörige IT-Komponenten sind in logischen Geschäftsservices wie E-Mail, Internetzugriff, Auftragserfassung, Finanzen usw. korreliert.

SPECTRUM Service Manager überbrückt die Lücke zwischen dem Betrieb und den Kundendienst-Service-Desks, indem Probleme hinsichtlich der Infrastrukturzuverlässigkeit mit den betroffenen Services und Kunden korreliert werden. Dadurch können Ressourcen je nach Priorität der betroffenen Services zugewiesen werden. Echtzeitalarme werden generiert, um vor Serviceausfällen und drohenden SLA-Verstößen unter Angabe der Ursache zu warnen, so dass rasch Korrekturmaßnahmen ergriffen werden können, bevor das Unternehmen gravierend beeinträchtigt wird. Ein Service-Dashboard ermöglicht einen Überblick über den Systemzustand. In Verlaufsberichten werden die früheren Leistungen sowie Details zu Verschlechterungen und Ausfällen aufgeführt, so dass Unternehmen im Laufe der Zeit neue Verfahren finden können, um die Services zu verbessern.

Service Manager umfasst die folgenden wichtigen Funktionen:

- proaktives Management von Unternehmensservices und SLAs
- intuitives Servicestatus-Dashboard
- webbasierte Service-Level-Berichte
- eine gleichzeitige Service-Dashboard-Lizenz
- Verwaltung mehrerer Services über zusätzliche SPECTRUM Assurance Servers

Komponenten des Sprachmanagements

Das Produkt eHealth for Voice umfasst die folgenden Komponenten:

Erforderliche Komponenten	Optionale Komponenten
eHealth for Voice Nutzungsrechtlizenz (pro PBX/Nachrichtensystem) Knotenlizenz (1 pro Anruf-/Nachrichtensystem)	eHealth for Voice Policy Manager

eHealth for Voice

eHealth for Voice ist eine Lösung für Leistungsmanagement, die mehrere Hersteller, Systeme (Anrufmanagement und Voice-Messaging) und Technologien (herkömmliche PBX (TDM) und IPT) berücksichtigt und das Management von Sprachnetzwerken erheblich vereinfacht. Mit eHealth for Voice entfallen die manuelle Datenerfassung sowie die arbeitsaufwändige Berichtskompilierung und Ermittlung der Verkehrsgüte (GoS, Grade of Service) für die Telefonie. Dies ermöglicht eine Verbesserung der Leistung und der Verfügbarkeit des Sprachsystems bei geringeren Kosten. Zudem ist eHealth for Voice eine Lösung, die keine Agenten verwendet und keine Softwareinstallation in den Sprachsystemen erfordert, wodurch die Installation vereinfacht und die Wertschöpfung beschleunigt wird.

Sie können viele verschiedene Berichte ausführen und an Drucker, E-Mail-Empfänger oder das Intranet weiterleiten. Mit eHealth for Voice sind präzise aktuelle und historische Systeminformationen für Trend- und Analysefunktionen stets verfügbar. Anstelle fragmentierter Daten-Snapshots werden exakte Leistungsmessungen täglich und automatisch für Desktops oder Drucker bereitgestellt.

Die Architektur von eHealth for Voice bietet maximale Skalierbarkeit durch die Modularisierung der Funktionen. Bei kleineren Installationen kann ein einzelner Server die Datenbank und das Datensammlungsmodul bereitstellen. Bei größeren Anwendungen können beliebig viele zusätzliche Server an verschiedenen Standorten als Datensammlungsagenten eingesetzt werden, die Daten aus Clustern herunterladen und an die zentrale Datenbank senden. Die Daten können nach einem benutzerdefinierten Zeitplan rund um die Uhr gesammelt werden, so dass der Abruf der Daten erfolgt, bevor sie überschrieben werden. Auf die zentrale Datenbank können beliebig viele Client-Computer über ein IP-Netzwerk zugreifen, das den Zugriff auf die Daten und Berichte ermöglicht.

Sie können eHealth for Voice kaufen, indem Sie die eHealth for Voice-Nutzungsrechtlizenz für die zu überwachende PBX oder das zu überwachende Anrufsystem bzw. Messaging-System bestellen (z. B. kaufen Sie CA eHealth for Voice – Nortel CS-1000 und Meridian für die Überwachung der Nortel-PBXs) und dann die entsprechende Anzahl der Knotenlizenzen erwerben. Für jedes überwachte Anruf- oder Messaging-System ist eine Knotenlizenz erforderlich.

eHealth for Voice Policy Manager

eHealth for Voice Policy Manager ist eine Komponente, die auf der eHealth for Voice-Engine eingesetzt wird, um alle Datenaktivitäten anhand benutzerdefinierter Kriterien zu überwachen und automatisch eine Benachrichtigung zu übermitteln, sobald diese Kriterien erfüllt werden. Dieses Modul ermöglicht Ihnen, bestimmte Schwellenwerte und Bedingungen für Knoten, die Plattform oder das gesamte System festzulegen und Benachrichtigungsaktionen zu definieren (u. a. E-Mail-, Konsolen- und Pager-Nachrichten senden, SNMP-Traps an SPECTRUM, an Unicenter NSM oder an Überwachungssysteme eines Drittherstellers übermitteln), wobei benutzerdefinierte Befehle und Skripts aufgerufen werden. Die Bedingungen werden mit einer oder mehreren Aktionen kombiniert, um Richtlinien zu erstellen. Der Policy Manager-Dienst, der auf dem eHealth for Voice-Anwendungsserver ausgeführt wird, überwacht die Daten beim Laden in die Datenbank anhand der aktiven Richtlinien und löst bei Bedarf automatisch Richtlinienaktionen aus. Sie können Policy Manager kaufen, indem Sie die Nutzungsrechtlizenz für eHealth for Voice – Policy Manager und dann die benötigte Anzahl der Knotenlizenzen bestellen. Für jedes überwachte Anruf- oder Messaging-System ist eine Knotenlizenz erforderlich.

Implementierungsarchitekturen

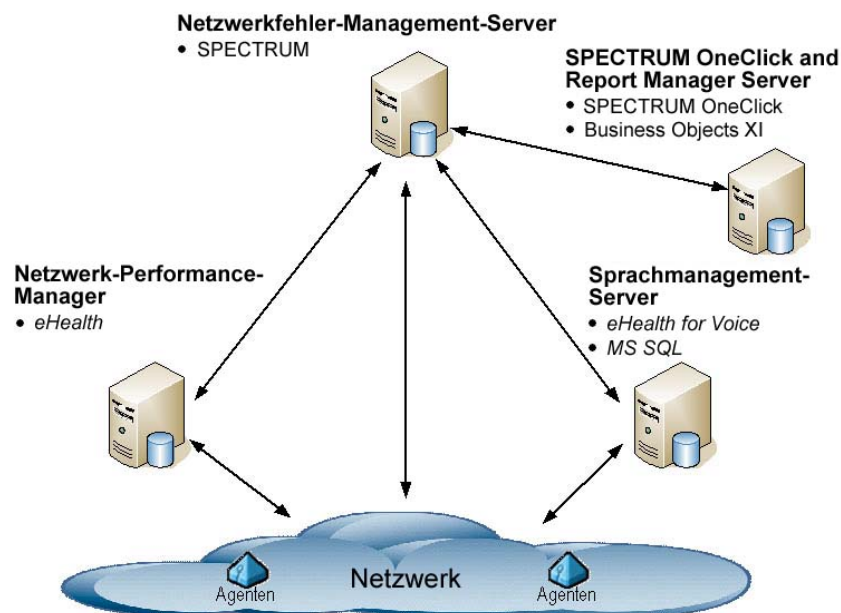
Die CA-Lösung für Netzwerk- und Sprachmanagement bietet zwei häufig verwendete Implementationen:

- kleine oder mittlere Implementationen mit einem zentralen Verwaltungsstandort und begrenzten verwalteten Ressourcen (unter 100.000) in einem kleinen geographischen Gebiet
- große Implementationen mit mehreren verteilten Verwaltungsstandorten und sehr vielen verwalteten Ressourcen in einem großen geographischen Gebiet

In den folgenden Abschnitten werden zwei Beispielimplementationen erläutert: eine kleine oder mittlere lokale Implementation, die für kleinere Unternehmen geeignet ist, sowie eine große und verteilte Implementation, die für einen großen Serviceanbieter eingesetzt werden kann. CA-Lösungen können viele verschiedene Implementationen und Geschäftsdienste unterstützen. Je größer die Umgebung, desto wichtiger ist der effektive Einsatz von CA Technology Services für die Planung, Implementation und Verwaltung der Lösung.

Implementation für kleine und mittelständische Unternehmen

In der Regel werden in einer Implementation für ein kleines oder mittelständisches Unternehmen alle Performance-Komponenten verwendet, die in diesem Kapitel vorgestellt werden, mit Ausnahme der Produkte Distributed eHealth und Remote Polling. Kleine und mittlere Implementationen werden gewöhnlich für Kunden mit 50.000 oder weniger verwalteten Ressourcen verwendet, die meist in einem begrenzten geographischen Gebiet verteilt sind. In Kapitel 5 werden die Best Practices sowie die erforderlichen Schritte für die Implementierung von kleinen und mittleren Implementationen erläutert. In der folgenden Grafik wird die Architektur einer Implementation für kleine und mittelständische Unternehmen dargestellt.



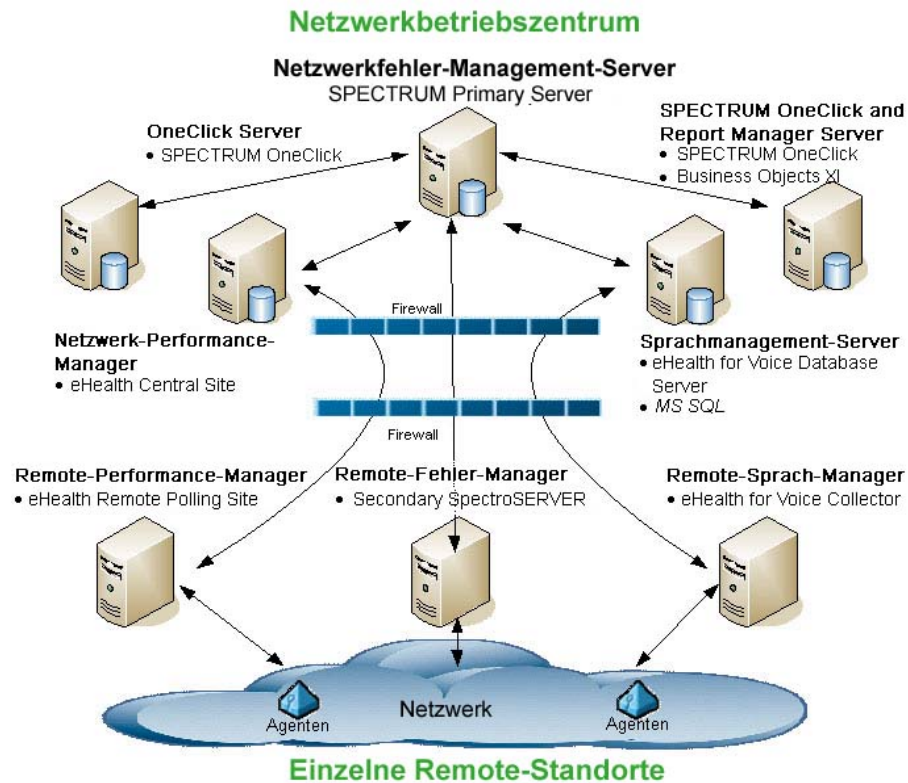
In der Regel werden in einer kleinen oder mittelgroßen Umgebung SPECTRUM, eHealth und eHealth for Voice in unabhängigen und dedizierten Systemen installiert. Zudem sollten die Anwendungen SPECTRUM OneClick und Report Manager ebenfalls in dedizierten Systemen installiert werden.

Implementation für große Serviceanbieter

In der Regel werden in einer Implementation für große Serviceanbieter alle Komponenten einschließlich der verteilten Konfigurationen verwendet, z. B. Distributed eHealth, eHealth Remote Polling, Distributed SpectroSERVER und verteilte Voice-Installationen. Große Implementationen werden gewöhnlich für Kunden mit Hunderttausenden oder mehr verwalteten Ressourcen verwendet, welche über ein großes geographisches Gebiet verteilt sind. Zudem müssen Serviceanbieter segmentierte Ansichten der Managementressourcen sicherstellen, da die Ressourcen möglicherweise unabhängigen Kunden „gehören“ oder zugewiesen sind.

In diesem Handbuch wird nicht die Planung und Konfiguration einer großen Implementation erläutert. Wenn Sie eine große Implementation planen, sollten Sie die Konfiguration zusammen mit Ihrem CA Sales and Technology Services-Team auf der Grundlage der Größe und Eigenschaften Ihres Netzwerks planen und implementieren.

In der folgenden Grafik wird die Architektur einer Implementation für einen großen Serviceanbieter dargestellt.



Die CA-Lösung für Netzwerk- und Sprachmanagement ist für die Unterstützung solcher großer Konfigurationen skalierbar. Wie in der Abbildung gezeigt, werden zentrale Systeme gewöhnlich im Bereich des primären Netzwerkbetriebszentrums (NOC, Network Operations Center) installiert. Sie können Systeme installieren, um Daten aus Bereichen zu sammeln, die näher an den Remote-Standorten liegen, in denen sich die verwalteten Ressourcen befinden. Das Remote-System und das zentrale System kommunizieren miteinander, um Informationen auszutauschen. Die CA-Lösung bietet viele verschiedene Möglichkeiten für die Verteilung der Managementdeckungs- und Abfragedienste sowie der Berichtsdienste, so dass viele verschiedene Managementumgebungen abgedeckt werden.

Dimensionierung sowie Hardware- und Softwareanforderungen für Netzwerkleistungen

Verwenden Sie eHealth Sizing Wizard, um die Anforderungen der Umgebung zu ermitteln. Sie können eHealth Sizing Wizard über die Website <http://www4.concord.com/sizing/swiz> aufrufen. Nachstehend werden die Mindestanforderungen für die Software und Hardware aufgelistet:

Technische Spezifikationen für eHealth 6.0 eHealth E2E Console erforderlich		
	UNIX	Windows
Mindestsystemanforderungen	Sun- oder HP-Server mit mindestens 900-MHz-CPU(s)	Server mit mindestens 2,0-GHz-CPU(s)
Betriebssysteme	Solaris 9, 10 (32- und 64-Bit)	Windows 2003: Standard, Enterprise
	HP-UX 11.i, 11.23 (64-Bit)	
Windows-Manager	OpenWindows, OSF/Motif, CDE	
Arbeitsspeicher	3 GB	3 GB
Auslagerungsbereich	6 GB	6 GB
Freier Festplattenspeicher	14 GB (berücksichtigt eHealth-Dateien, Oracle, Datenbank und Speicherort für die DB-Sicherung)	(NTFS Format) 14 GB (berücksichtigt eHealth-Dateien, Oracle, Datenbank, Anwendungen von Drittherstellern und Speicherort für die DB-Sicherung)
	Bei Verwendung der optionalen Funktion Report Center müssen 50 % mehr freier Festplattenspeicher und 1 GB mehr Arbeitsspeicher berücksichtigt werden.	Bei Verwendung der optionalen Funktion Report Center müssen 50 % mehr freier Festplattenspeicher und 1 GB mehr Arbeitsspeicher berücksichtigt werden.
Web-Browser	Mozilla 1.6 (oder höher)	Mozilla 1.6 (oder höher)
		Internet Explorer 6 (oder höher)
		Mozilla FireFox 1.x

Dimensionierung sowie Hardware- und Softwareanforderungen für Network Fault Management

Verwenden Sie das Tool SPECTRUM Sizer, um zu ermitteln, wie viele SpectroSERVER für die effiziente Verwaltung Ihres Netzwerks erforderlich sind. Weitere Informationen über die Verwendung von SPECTRUM Sizer erhalten Sie beim Technischen Support oder bei Ihrem CA-Vertriebsbeauftragten. Nachstehend werden die Mindestanforderungen für die Software und Hardware aufgelistet:

Technische Spezifikationen für SPECTRUM 8.0		
	UNIX/Linux	Windows
Mindestsystemanforderungen	Sun UltraSPARC II Linux – Pentium Xeon	Pentium Xeon
Betriebssysteme	Solaris 9, 10 (erforderliche Patches s. Installationshandbuch)	Windows 2000, Windows XP Professional oder Windows 2003 Server
	Linux Red Hat Version 3, Update 6 oder höher	
Arbeitsspeicher	2 GB	2 GB
Freier Festplattenspeicher	40 GB	40 GB

Technische Spezifikationen für SPECTRUM Report Manager- und OneClick-Server		
	UNIX/Linux	Windows
Mindestsystemanforderungen	Sun SPARCstation Linux – Pentium Xeon	Pentium Xeon
Betriebssysteme	Solaris 9, 10 (erforderliche Patches s. Installationshandbuch)	Windows 2000, Windows XP Professional oder Windows 2003 Server
	Linux Red Hat Version 3, Update 6 oder höher	Hinweis: Business Objects XI unterstützt maximal 10 Benutzer unter XP.
Arbeitsspeicher	1 GB (mit 2 GB Auslagerungsbereich für Solaris)	1 GB
Freier Festplattenspeicher	4 GB	4 GB
Anwendungen	Linux Update 6 oder höher Solaris-Pakete SUNWeu8os SUNWeuluf	Informationen über Updates für Ihre Windows-Version erhalten Sie beim Microsoft-Support. Business Objects XI Service Pack 1

Technische Spezifikationen für SPECTRUM OneClick-Server (ohne Report Manager)		
	UNIX/Linux	Windows
Mindestsystemanforderungen	Sun SPARCstation Linux – Pentium Xeon	Pentium Xeon
Betriebssysteme	Solaris 9, 10 (erforderliche Patches s. Installationshandbuch)	Windows 2000, Windows XP Professional oder Windows 2003 Server
	Linux Red Hat Version 3, Update 6 oder höher	
Arbeitsspeicher	1 GB	1 GB
Freier Festplattenspeicher	230 MB	230 MB
Anwendungen	Linux Update 6 oder höher Java 2 SDK, Standard Edition, Version 1.5.0_06 oder höher	Windows 2000 – Service Pack 2 oder höher Java 2 SDK, Standard Edition, Version 1.5.0_06 oder höher

eHealth for Voice – Hardware- und Softwareanforderungen für Einzelplatzrechner und Datenbankserver

	Windows
Mindestsystemanforderungen	Pentium 1 GHz oder höher
Betriebssysteme	Windows 2000 Server Windows 2003 Server
Arbeitsspeicher	mindestens 512 MB, empfohlen 1 GB
Freier Festplattenspeicher	1 GB für die eHealth for Voice-Programmdateien
	5 bis 20 GB für Datenbank je nach Anzahl der Sprachplattformen und -systeme
Datenbanksoftware	Microsoft SQL Server 2000 mit Service Pack 2 oder höher, oder Microsoft SQL Server 2005 Hinweis: Muss vom Kunden separat gekauft und installiert werden.

Informationen zu den Hardware- und Software-Systemanforderungen für reine Anwendungs- und Client-Installationen finden Sie im *eHealth for Voice Operations Guide*.

(Diese Seite wurde absichtlich leer gelassen)

Kapitel 5: Einrichtung und Konfiguration der integrierten Lösung

In diesem Kapitel wird erläutert, wie die Komponenten der CA-Lösung für Netzwerk- und Sprachmanagement **in einer kleinen bis mittelgroßen Implementationsumgebung** installiert und konfiguriert werden. Darüber hinaus werden Best Practices für die Konfiguration der Komponenten zur Leistungsüberwachung beschrieben.

In diesem Handbuch wird nicht die Planung und Konfiguration einer großen Implementation erläutert. Wenn Sie eine große Implementationslösung planen, sollten Sie die Konfiguration zusammen mit Ihrem CA Sales and Technology Services-Team auf der Grundlage der Größe und Eigenschaften Ihres Netzwerks planen und implementieren.

Installation der CA-Lösungssoftware für Netzwerk- und Sprachmanagement

Um die integrierte Netzwerk- und Sprachmanagementumgebung zu implementieren, müssen Sie die Anwendungen SPECTRUM, eHealth und eHealth for Voice in Systemen installieren, die für die jeweiligen Anwendungen reserviert sind.

Wichtig: Die Installationsprozeduren für die jeweiligen Anwendungen werden detailliert in den produktspezifischen Installationshandbüchern erläutert, die in diesem Kapitel aufgeführt werden. **Sie müssen diese Handbücher verwenden, damit Sie die Anwendungen korrekt installieren können.** Lesen Sie zuerst dieses Kapitel, um sich mit den Best Practices zum Erstellen der integrierten Lösung mit diesen Anwendungen vertraut zu machen.

Installationsvoraussetzungen

Bevor Sie fortfahren, sollten Sie Kapitel 4 dieses Handbuchs lesen, um sicherzustellen, dass Ihre Systeme die grundlegenden Mindestanforderungen erfüllen und über die entsprechende Größe verfügen, die zur Unterstützung der Anwendungen in Ihrer Umgebung erforderlich ist. Wenn die Systeme nicht korrekt dimensioniert sind, können sie die mit den Anwendungen verbundenen Arbeitslasten nicht unterstützen. Dies kann dazu führen, dass sich die Leistung der CPUs, der Festplatten und des Arbeitsspeichers verschlechtert.

Hinweis: Das CA Sales-Team stellt sicher, dass Sie Ihre Systeme für die Unterstützung aller einzusetzenden Anwendungen sowie aller mit diesen Anwendungen zu verwaltenden Ressourcen korrekt dimensionieren.

Installationsschritte

Die Softwareanwendungen können in jeder beliebigen Reihenfolge installiert werden. Als Best Practice empfiehlt es sich, zuerst SPECTRUM und SPECTRUM OneClick/Report Manager zu installieren, dann eHealth und schließlich eHealth for Voice.

Wichtig: Die CA-Anwendungen für das Netzwerk- und Sprachmanagement erfordern die Verwendung von Systemen, die für jede Anwendung dediziert sind. Verwenden Sie diese Systeme **nicht** für andere Anwendungen oder Services. Obwohl die Verwendung von Antiviren- und Sicherheitsprogrammen für alle Serversysteme in Ihrer Umgebung empfohlen wird, sollten Sie die Antivirensoftware bei der Installation **deaktivieren**, um sicherzustellen, dass die Anwendungen vollständig installiert werden.

Sie benötigen mindestens vier Systeme für die folgende Basiskonfiguration:

- SPECTRUM (SpectroSERVER-System)
- SPECTRUM OneClick- und Report Manager-Server
- eHealth
- eHealth for Voice

BEST PRACTICES

Überprüfen Sie die folgenden Best Practices, um die Installation und Einrichtung dieser Komponenten zu vereinfachen:

- Stellen Sie sicher, dass die Systeme, in denen Sie die Software installieren möchten, feste IP-Adressen haben.
- Sorgen Sie dafür, dass Sie über die erforderlichen User-Berechtigungen für die Systeme verfügen, und testen Sie sie. Für Windows-Systeme benötigen Sie einen User mit Administratorrechten. Für UNIX-Systeme benötigen Sie einen „root“-User.

Installation von SPECTRUM

Installieren Sie in dem System, das Sie als SpectroSERVER für Ihre Umgebung vorgesehen haben, SPECTRUM Release 8.0. Melden Sie sich auf der Website <http://support.concord.com> an, um auf der Seite „Software Downloads“ das neueste Service Pack für das Release herunterzuladen.

Befolgen Sie die Anweisungen im *SPECTRUM Installation Guide*, um die folgenden Aufgaben durchzuführen:

1. Bestätigen Sie die SPECTRUM-Voraussetzungen.
2. Bereiten Sie das Betriebssystem vor, und optimieren Sie das System, um eine optimale Leistung zu ermöglichen.
3. Stellen Sie sicher, dass Sie über die Lizenz- und Extraktionsschlüssel für SPECTRUM verfügen. Die Schlüssel erhalten Sie beim Erwerb der Software von Ihrem CA-Vertriebsbeauftragten.
4. Installieren Sie die Software, und führen Sie bei Bedarf eine Problembehandlung für die Installation durch.
5. Starten Sie die SPECTRUM-Software.
6. Aktivieren Sie den Zugriff auf das SPECTRUM-System.

Wenn Sie die SPECTRUM-Installation abgeschlossen haben, fahren Sie mit der Installation von SPECTRUM OneClick fort. Installieren Sie OneClick, damit Sie vollständigen Administratorzugriff auf SPECTRUM haben.

Hinweis: OneClick ist die primäre Administrationsschnittstelle für SPECTRUM. Verwenden Sie für die Durchführung administrativer Aufgaben OneClick anstelle der veralteten SpectroGRAPH-Schnittstelle.

Installation von SPECTRUM OneClick und Report Manager

Installieren Sie SPECTRUM OneClick und Report Manager für Release 8.0 in dem System, das Sie als Server für OneClick und Report Manager für Ihre Umgebung vorgesehen haben.

Befolgen Sie die Schritte im Installationshandbuch *Report Manager Installation and Administration Guide*, um die folgenden Aufgaben durchzuführen:

Wichtig: Gehen Sie bei der Installation der OneClick- und Business Objects-Software genau nach der Anleitung in der Dokumentation vor. Installationsfehler werden in der Regel dadurch verursacht, dass die dokumentierten Schritte nicht eingehalten werden. Installieren Sie zuerst Business Objects, und wählen Sie die Option für die Verwendung eines vorhandenen Java-Anwendungsservers. Bei einem Fehler müssen Sie OneClick und Report Manager entfernen und erneut installieren.

1. Bestätigen Sie die Anforderungen und Systemvoraussetzungen für OneClick.
2. Bereiten Sie das Betriebssystem vor, und optimieren Sie die Systemparameter, um eine optimale Leistung zu ermöglichen.
3. Installieren Sie die Software, und führen Sie bei Bedarf eine Problembehandlung für die Installation durch.
4. Installieren Sie den OneClick-Client zum Ausführen der Anwendung, und bestätigen Sie, dass Sie eine Verbindung zum SpectroSERVER-System herstellen können.
5. Klicken Sie auf der OneClick-Indexseite der OneClick-Benutzeroberfläche auf die Registerkarte „Report Manager“, um zu bestätigen, dass Report Manager korrekt installiert wurde.

Installation von eHealth

Installieren Sie eHealth Release 6.0 in dem System, das Sie als eHealth-Server vorgesehen haben. Melden Sie sich auf der Website <http://support.concord.com> an, um das neueste InstallPlus-Kit für das Release von der Seite „Software Downloads“ herunterzuladen.

Befolgen Sie die Anweisungen im Installationshandbuch *New Installations of eHealth 6.0 Guide* für Ihre Systemplattform (Windows oder UNIX), um die folgenden Aufgaben durchzuführen:

1. Bestätigen Sie die Systemvoraussetzungen und Speicherorte für die eHealth- und integrierte Oracle-Software.
2. Installieren Sie die eHealth- und Oracle-Software, und führen Sie bei Bedarf eine Problembehandlung für die Installation durch.
3. Stellen Sie sicher, dass Sie über die erforderlichen eHealth-Lizenzen für die Funktionen verfügen, die Sie verwenden möchten. Sie erhalten diese Lizenzen beim Kauf der eHealth-Produkte. Beachten Sie, dass Sie für eHealth Release 6.0 GA eine Lizenz für eHealth SPECTRUM Integration benötigen, um die integrierte Lösung konfigurieren und verwenden zu können.

Wichtig: Nachdem Sie die eHealth-Installation abgeschlossen haben, befolgen Sie die Anweisungen des Abschnitts „Konfiguration der integrierten Lösung“ in diesem Kapitel. **Befolgen Sie nicht** die Anweisungen zum Starten der eHealth-Konsole für die Discovery Ihrer Ressourcen als Elemente. Bei der integrierten Lösung werden die eHealth-Elemente erkannt, indem die SPECTRUM-Konfiguration aus dem SpectroSERVER-System importiert wird. Dadurch werden die Administrationsaufgaben für die eHealth-Discovery vereinfacht. Eine Beschreibung der eHealth-Administrationsaufgaben und -schnittstellen finden Sie im *Health Administration Overview Guide*.

Installation von eHealth for Voice

Installieren Sie eHealth for Voice Release 4 in dem System, das Sie als eHealth for Voice-Server vorgesehen haben. Sie können eHealth for Voice komplett auf einem PC installieren. Sie können die Software auch in einer verteilten Umgebung auf mehreren PCs installieren. Hierbei dient ein PC als Datenbankserver, während die anderen als Clientsysteme verwendet werden, die über den Datenbankserver auf Berichte und Administrationsaufgaben zugreifen können.

Für den Database Manager-Server ist eine Microsoft SQL Server-Datenbank-Engine erforderlich. Vor der Installation von eHealth for Voice müssen Sie ggf. Microsoft SQL Server kaufen und installieren. In der Regel wird Microsoft SQL Server 2000 auf dem PC installiert, auf dem die eHealth-Datenbank abgelegt werden soll.

Hinweis: Microsoft SQL Server ist nur auf dem PC erforderlich, auf dem die eHealth for Voice-Datenbank gespeichert werden soll (die Database Manager-Installation) und wird auf reinen Agenten- oder Client-Computern nicht benötigt.

Befolgen Sie die Anweisungen im *eHealth for Voice Operations Guide*, um die folgenden Aufgaben durchzuführen:

1. Bestätigen Sie die Systemvoraussetzungen.
2. Installieren Sie die Software, und führen Sie bei Bedarf eine Problembehandlung für die Installation durch.
3. Optional können Sie clientseitige Server installieren, um auf den eHealth for Voice-Datenbankserver zuzugreifen.
4. Starten Sie die Programmkonsole, und definieren Sie Ihre Sprachumgebung:
 - a. Installieren Sie die Lizenzen für die Plattformen, die unterstützt werden sollen.
 - b. Starten Sie (mindestens) die folgenden Dienste:
 - > Task Scheduler
 - > Data Collector
 - > Data Loader
 - > Policy Manager

- c. Definieren Sie folgende Elemente:
 - > Company
 - > Group
 - > Collector
 - > Platform
 - d. Markieren Sie die Warteschlange „Data Collection“, um die geplante Datensammlung zu prüfen.
5. Richten Sie die SPECTRUM-Integration ein, indem Sie die Anweisungen im *eHealth for Voice Integration for SPECTRUM Guide* befolgen.

Nachdem Sie die eHealth for Voice-Installation abgeschlossen haben, befolgen Sie die Anweisungen zum Starten der Programmkonsole, und definieren Sie Ihre Sprachumgebung. Richten Sie dann die SPECTRUM-Integration ein, indem Sie die Anweisungen im *eHealth for Voice Integration for SPECTRUM Guide* befolgen.

Konfiguration der integrierten Lösung

Mit SPECTRUM, SPECTRUM OneClick, eHealth und eHealth for Voice können Sie eine integrierte Lösung für die Verwaltung von Netzwerk- und Sprachressourcen bereitstellen.

- SPECTRUM stellt die Top-Level-Managementschnittstelle zur Ressourcenidentifikation, zum Fehlermanagement und zur Lösung von IT-Netzwerkproblemen bereit. Mit SPECTRUM können akustische Alarmsignale verringert und die Ursachen von Problemen erkannt werden.
- eHealth ermöglicht Performance-Management, indem detaillierte statistische Daten zu den Ressourcen gesammelt und diese Daten anschließend analysiert werden, um wachsende Probleme und Änderungen des Verhaltens frühzeitig zu erkennen. eHealth Live Health vergleicht die Leistung mit Schwellenwerten und Serviceregeln und löst Alarme aus, sobald sich die Ressourcenleistung verschlechtert. Health-Berichte und Live Health können Alarme (Traps) an SPECTRUM übermitteln, so dass die Probleme in OneClick-Ansichten berücksichtigt werden.
- eHealth for Voice verwaltet den End-to-End-Service sowohl für herkömmliche Sprachnetzwerke als auch für konvergente VoIP-Netzwerke. Es kann Verstöße gegen die Servicerichtlinien und Kapazitätsprobleme erkennen und Alarme an SPECTRUM senden, damit Netzwerkmanager über die OneClick-Ansichten eine Warnung erhalten.

Diese Produkte können separat verwendet werden, um die Netzwerkleistung und Fehler zu verwalten sowie Berichte zu erstellen. Die kombinierte Verwendung der Produkte ermöglicht Netzwerkmanagern, in einer einzigen Ansicht auf oberster Ebene einen Überblick über potenzielle Probleme und Änderungen hinsichtlich der Netzwerkleistung zu erhalten und bei Bedarf über Berichte Detailinformationen und Informationen zur Problembehandlung abzurufen.

Best Practices

In den folgenden Abschnitten werden die Best Practices für die Konfiguration der integrierten CA-Lösung für Netzwerk- und Sprachmanagement erläutert. Die Best Practices ermöglichen eine Rationalisierung häufiger Administrationsaufgaben und verringern den Zeitaufwand für die Verwaltung und Wartung der Softwarekonfigurationen.

Führen Sie die folgenden grundlegenden Schritte aus, um die integrierte Lösung zu konfigurieren:

1. Identifizieren Sie mit Hilfe der SPECTRUM-Discovery die Netzwerkressourcen, die verwaltet werden sollen. Erstellen Sie anschließend Global Selections, um diese Ressourcen zu strukturieren.
2. Importieren Sie die von SPECTRUM erkannten Ressourcen in eHealth, indem Sie den Discovery-Prozess von eHealth verwenden.
3. Vereinfachen Sie das Reporting und das Management von Ressourcen, indem Sie zusammengehörige Elemente auf der Grundlage der Beziehungen (wie geographische Region, Kunde, Organisation oder Abteilung) in Gruppen und Gruppenlisten zusammenfassen, die sie unterstützen.
4. Planen Sie die eHealth-Discovery von Global Selections für die Pflege der Poller-Konfiguration.

In den folgenden Abschnitten werden diese Schritte detaillierter erläutert und Verweise auf die Produktdokumentation bereitgestellt, in der Sie vollständige Informationen zu den beschriebenen Themen finden.

Identifizierung von Ressourcen und deren Discovery (Erkennung) als Global Selections mit Hilfe von SPECTRUM

Identifizieren Sie mit Hilfe der SPECTRUM-Discovery die Netzwerkressourcen, die verwaltet werden sollen, und erstellen Sie dann Global Selections, um die Ressourcen in Topologieansichten zu strukturieren. Netzbetreiber können mit diesen Ansichten verschiedene Sammlungen von Netzwerkentitäten, Organisationen oder Services verfolgen, die Ihre Infrastruktur enthalten.

Außerdem nutzt die eHealth-Discovery Global Selections als Input. Nachstehend wird schrittweise erläutert, wie eine statische Sammlung von Elementen quasi „nebenbei“ erstellt wird. SPECTRUM bietet viele verschiedene Arten der Discovery sowie unterschiedliche Herangehensweisen. Informationen über die Ermittlung des effektivsten Ansatzes für Ihre Organisation finden Sie im *Modeling Your IT Infrastructure Administrator Guide* und im *AutoDiscovery User Guide*.

So erstellen Sie eine neue Sammlung:

1. Melden Sie sich bei der SPECTRUM OneClick-Konsole an, und wählen Sie „Tools“, „Utilities“, „Discovery“ und „New Discovery“.
2. Führen Sie im Dialogfeld „Discovery“ die folgenden Schritte aus:
 - a. Geben Sie einen Konfigurationsnamen an.
 - b. Geben Sie einen IP-Adressenbereich oder eine IP-Adressenliste an, oder importieren Sie eine Datei.
 - c. Geben Sie eine gültige Community-Zeichenfolge ein.
 - d. Wählen Sie unter „Modeling Options“ die Option „Discover Only“.
 - e. Klicken Sie auf „Discover“.

- f. Wenn das Ergebnis angezeigt wird, identifizieren Sie Geräte, die nicht überwacht werden sollen. Klicken Sie mit der rechten Maustaste auf diese Geräte, und wählen Sie „Exclude“, um sie auszuschließen.
 - g. Wählen Sie „Model“.
 - h. Wählen Sie die gewünschten Modellierungsoptionen.
 - i. Klicken Sie auf „OK“.
 - j. Klicken Sie auf „Close“.
 - k. Wählen Sie „Yes“, um die Discovery Configuration zu speichern.
 - l. Wählen Sie „Cancel“, um das Dialogfeld „Discovery“ zu schließen.
3. Wechseln Sie im OneClick-Navigationsbereich zur Registerkarte „Locator“, und verwenden Sie eine Suchoption, um anhand bestimmter Kriterien (z. B. IP-Adresse oder Modellname) nach Ressourcen zu suchen.
 4. Wählen Sie ein oder mehrere Elemente aus. Klicken Sie mit der rechten Maustaste auf die jeweiligen Elemente, und wählen Sie „Add To“ und „Collections“.
 5. Klicken Sie im Dialogfeld „Select Collections“ auf „Create“.
 6. Geben Sie einen Namen und eine Beschreibung für die Sammlung an, und klicken Sie auf „OK“.
 7. Klicken Sie auf „OK“.

Sie können diesen Prozess in regelmäßigen Abständen ausführen, damit die Konfiguration stets auf dem neuesten Stand ist.

Importieren von Global Selections in eHealth

Importieren Sie die von SPECTRUM erkannten Ressourcen in eHealth, indem Sie die Discovery-Funktion von eHealth verwenden. Dadurch beginnt eHealth automatisch, Ressourcen abzufragen und auf diese Weise für sie eine Performance-Datenbank und einen Performance-Verlauf zu erzeugen. Auf der Grundlage dieser Performance-Datenbank können eHealth-Berichte und Live Health Änderungen im Verhalten feststellen, potenzielle Service- oder Kapazitätsprobleme identifizieren und Informationen zu den Performance-Trends im Zeitverlauf bereitstellen.

EINRICHTUNG DER SPECTRUM-INTEGRATION

Bevor Global Selections in eHealth importiert werden können, müssen Sie das SPECTRUM-Setup-Programm im eHealth-System ausführen.

So führen Sie das Setup-Programm für die eHealth SPECTRUM-Integration aus:

1. Melden Sie sich beim eHealth-System als eHealth-Administrator an.
2. Öffnen Sie ein Terminalfenster, und wechseln Sie zum eHealth-Verzeichnis, indem Sie den folgenden Befehl eingeben, wobei *ehealth* der vollständige Pfadname ist:

```
cd ehealth
```

3. Führen Sie das Setup-Programm aus, indem Sie den folgenden Befehl eingeben:

`./bin/nhSPECTRUMSetup`

Das Dialogfeld „**SPECTRUM** Import Setup“ wird angezeigt.

4. Geben Sie die folgenden Informationen ein, wenn Sie vom Setup-Programm dazu aufgefordert werden:
 - > Hostname oder IP-Adresse des **SPECTRUM** OneClick-Servers
 - > Portnummer für Webanforderungen des OneClick-Servers
 - > Installationspfad für OneClick auf dem Server
 - > Benutzername für die Anmeldung beim OneClick-Server
 - > Kennwort für den angegebenen Benutzernamen
5. Klicken Sie auf „OK“. eHealth überprüft Ihre Einstellungen und zeigt in einer Meldung an, ob diese gültig sind.

Hinweis: Der Validierungsvorgang dauert möglicherweise einige Sekunden.

DISCOVERY VON GLOBAL SELECTIONS IN SPECTRUM

Verwenden Sie die eHealth-Discovery, um die SPECTRUM-Konfiguration in eHealth zu importieren.

So erkennen Sie eine Global Selection in SPECTRUM:

1. Melden Sie sich bei der eHealth-Konsole an.
2. Wählen Sie „Setup“ und „Discover“.
3. Führen Sie im Dialogfeld „Discover“ die folgenden Schritte aus:
 - a. Wählen Sie aus der Liste „Mode“ die Technologietypen, die den zu erkennenden Ressourcen zugeordnet sind.
 - b. Wählen Sie „SPECTRUM Import“. Geben Sie die globale SPECTRUM-Sammlung an, die importiert werden soll.
 - c. Klicken Sie auf „Discover“.

eHealth stellt eine Verbindung mit dem OneClick-Server her, extrahiert die Informationen aus der SPECTRUM-Sammlung und erkennt die entsprechenden Elemente.

4. Speichern Sie die erkannten Elemente in der Poller-Konfiguration. eHealth beginnt den Datenabruf automatisch, um Performance-Daten zu sammeln.

Strukturierung von Ressourcen durch Erstellung von eHealth-Gruppen

eHealth bietet eine Gruppierungsfunktion, mit der Sie Elemente effizient strukturieren sowie die Administration und Berichtverfassung vereinfachen können. Indem Sie sich nur auf eine Teilgruppe von Elementen konzentrieren, anstatt alle Elemente in der Infrastruktur zu berücksichtigen, können Sie diese einfacher verwalten und gezielt effektive Berichte für bestimmte Anforderungen erstellen. Zur Verwaltung der Infrastruktur können Sie zusammengehörige Elemente nach den von ihnen unterstützten geographischen Regionen, Kunden, Organisationen oder Abteilungen in Gruppen zusammenfassen. Sie können die Gruppen strukturieren, indem Sie sie Gruppenlisten zuordnen.

Wenn Sie beispielsweise die Systeme überwachen möchten, die Ihr Unternehmen in Europa unterstützen, können Sie für jedes Land, in dem Ihr Unternehmen aktiv ist, eine Gruppe (mit allen Ressourcen, die Niederlassungen im betreffenden Land unterstützen) erstellen, z. B. die Gruppe „England“. Anschließend können Sie diese Gruppen in einer Gruppenliste mit dem Namen „Europa“ zusammenfassen und für die gesamte Gruppenliste Berichte generieren. Sie können außerdem die Elementlisten anhand Ihrer Gruppierungsstrategie filtern, um die Berichtverfassung und Administration zu vereinfachen. Bevor Sie Ressourcen gruppieren, sollten Sie sich mit den Best Practices von eHealth für die Gruppierung vertraut machen, die im *eHealth Element and Poller Management Guide* erläutert werden.

So erstellen Sie eine neue Gruppe:

1. Melden Sie sich bei der OneClick for eHealth-Konsole als Administrator an, der zur Verwaltung von Gruppen berechtigt ist.
2. Wählen Sie im Ordner „Managed Resources“ die Option „Find Elements“.
3. Wählen Sie die Elemente aus, die in der Gruppe enthalten sein sollen. Wählen Sie „Element Chooser“, um die Liste zu filtern. Sie können Wildcards verwenden, z. B. ein Sternchen (*) für mehrere Zeichen oder ein Fragezeichen (?) für ein einzelnes Zeichen.
4. Klicken Sie mit der rechten Maustaste, und wählen Sie „Create Group with Selected Elements“.
5. Geben Sie den ersten Gruppennamen und eine Beschreibung ein. Falls SmartTree aktiviert ist, hängen Sie eine Bezeichnung an den Gruppennamen an, der den Standort der Elemente angibt, und verwenden Sie den ausgewählten Delimiter (z. B. England-1, Deutschland-1 oder Spanien-1).
6. Klicken Sie auf „OK“. Die Gruppe wird sofort unter „By Group“ angezeigt.
7. Wiederholen Sie die Schritte 2 bis 6, um weitere Gruppen mit einem Suffix zu erstellen. Beispiel: England-2, Deutschland-2, Spanien-2.
8. Wählen Sie unter „Managed Resources“ die Option „By Group“. Wenn SmartTree aktiviert ist, zeigt die Elementstruktur zwei Ebenen in einer alphabetisch geordneten Hierarchie auf Basis der Benennungskonvention an.

So fügen Sie einer Gruppenliste Gruppen hinzu:

1. Melden Sie sich bei der OneClick for eHealth-Konsole als Administrator an, der zur Verwaltung von Gruppen berechtigt ist.
2. Klicken Sie mit der rechten Maustaste im Ordner „Managed Resources“ auf „By Group List“, und wählen Sie „New Group List“.
3. Geben Sie einen Namen und eine Beschreibung ein, und klicken Sie auf „OK“.
4. Doppelklicken Sie auf den unter „By Group List“ angezeigten Gruppenlistenamen, und wechseln Sie zur Registerkarte „Groups Not in This Group List“.
5. Wählen Sie die Gruppen aus, die in die Liste aufgenommen werden sollen. Klicken Sie mit der rechten Maustaste, und wählen Sie „Add Selected Groups to Group List“.
6. Klicken Sie zum Bestätigen auf „Yes“.
7. Klicken Sie auf „OK“, um zu speichern.

Planung der eHealth-Discovery von Global Selections

Sie können die eHealth-Discovery von Global Selections planen, damit die Elementdefinitionen in der Poller-Konfiguration stets auf dem neuesten Stand sind. Ein geplanter Job für die Discovery wird automatisch ausgeführt, um die Elementinformationen zu aktualisieren und sicherzustellen, dass die überwachten Elemente auf eHealth-Pollings reagieren.

So planen Sie die Discovery:

1. Melden Sie sich bei der eHealth-Konsole an.
2. Wählen Sie „Setup“ und „Schedule Jobs“.
3. Wählen Sie im Dialogfeld „Schedule Job“ aus der Liste „Add“ den Eintrag „Add Discover“. (Die Standardeinstellung für die Liste „Add“ ist „Add At-a-Glance“.)
4. Führen Sie im Dialogfeld „Add Scheduled Discover Job“ die nachstehend erläuterten Schritte aus, und klicken Sie dann auf „Schedule“:
 - a. Wählen Sie unter „Mode“ einen oder mehrere Elementtypen aus.
 - b. Wählen Sie „SPECTRUM Import“, und geben Sie die Global Selection an.
 - c. Legen Sie fest, an welchen Tagen und zu welcher Uhrzeit die geplante Discovery ausgeführt werden soll. Als Best Practice empfiehlt es sich, die geplante eHealth-Discovery nach den SPECTRUM AutoDiscovery-Aktualisierungen auszuführen, damit die Konfigurationen stets synchronisiert sind. Wenn sich die Umgebung nicht oft ändert, können Sie bei der Planung der Rediscovery größere Zeitabstände festlegen. Wenn die Umgebung sehr dynamisch ist, müssen Sie häufigere Rediscoveries einplanen, um sicherzustellen, dass die Konfigurationen stets aktuell sind.
 - d. Klicken Sie auf „Schedule“.
 - e. Klicken Sie auf „OK“.

Netzwerk- und Sprachüberwachung

Mit der integrierten CA-Lösung können Sie die Leistung der Netzwerk- und Sprachressourcen genau überwachen. Die Anwendung eHealth Live Health gibt bei Problemen sofort Rückmeldung und informiert Sie darüber, wo die Probleme aufgetreten sind, wann sie begonnen und welchen Schweregrad sie haben. Zudem identifiziert sie wachsende Probleme, bevor diese zu Fehlern werden. Auf diese Weise können Sie rechtzeitig Maßnahmen ergreifen und den reibungslosen Betrieb des Unternehmens aufrechterhalten. Live Exceptions sendet Alarmbenachrichtigungen an die SPECTRUM-Schnittstelle. Sie können anschließend Berichte aus der SPECTRUM OneClick-Schnittstelle ausführen, um die eHealth-Analysen der Probleme durchzusehen.

Führen Sie die folgenden grundlegenden Schritte aus, um die integrierte Lösung für die Leistungsüberwachung zu konfigurieren:

1. Richten Sie die Live Health-Überwachung von eHealth-Gruppen und -Gruppenlisten ein.
2. Leiten Sie Live Health-Traps an SPECTRUM weiter.
3. Sie können Health-Berichte auch individuell anpassen und deren Ausführung planen, um Traps an SPECTRUM zu senden.
4. Konfigurieren Sie eHealth for Voice zum Senden von Alerts an SPECTRUM.
5. Konfigurieren Sie SPECTRUM zur Discovery (Erkennung) des eHealth-Servers.
6. Konfigurieren Sie SPECTRUM zum Anzeigen von eHealth-Alarmen.

In den folgenden Abschnitten werden diese Schritte detaillierter erläutert und Verweise auf die Produktdokumentation bereitgestellt, in der Sie vollständige Informationen zu den beschriebenen Themen finden.

Einrichtung von Live Health

Nachdem Sie die Discovery und Gruppierung der zu überwachenden Ressourcen abgeschlossen haben, können Sie sie einem Live Health-Profil zuordnen, um anzugeben, wann Performance-Probleme vorliegen. Bei einem Live Health-Profil handelt es sich um einen Satz von Alarmregeln, den eHealth auf Elementgruppen oder -gruppenlisten anwendet. Alarmregeln definieren die Arten der zu überwachenden Elemente und Bedingungen sowie die Schwellenwerte, die Dauer und den Schweregrad des Problems.

eHealth stellt mehrere Hundert technologiespezifische Profile für die Verwaltung von Netzwerkressourcen bereit. Für die einzelnen Technologien stellt eHealth jeweils die folgenden Live Health-Profiltypen bereit:

Profilname	Verwendungszweck
Failure	Identifiziert Probleme im Zusammenhang mit Verfügbarkeit, Fehlern oder anderen Gerätedefekten.
Delay	Warnt vor Problemen durch übermäßige Auslastung oder Überlastung, die zu Verzögerungen im Netzwerk führen können.
Unusual workload	Gibt an, wenn die Kapazität oder das Volumen eines Elements außerhalb der typischen Performance für die Baseline liegt.
Latency	Identifiziert eine Verlangsamung der Wartezeit im Netzwerk. Die Wartezeit wird in der Regel zwischen dem eHealth-System und dem Gerät gemessen.
Configuration change	Erkennt Änderungen an der Konfiguration eines Geräts, z. B. die Hinzufügung eines Moduls oder einer Karte zu einem Switch.
Security	Warnt vor Sicherheitsproblemen, z. B. wenn eine Firewall einen Ping-of-Death-Angriff, Anmeldefehler oder nicht autorisierte Zugriffe erkennt.

Nachdem Sie einer Elementgruppe oder -gruppenliste ein Profil zugeordnet haben, werden diese von Live Exceptions überwacht. Live Exceptions prüft, ob Aktivitäten gegen die Regeln verstoßen, die für das Profil angegeben sind, und generiert bei einem Verstoß entsprechende Alarme. Mit Hilfe dieser integrierten Lösung können Sie Live Health so konfigurieren, dass im Falle von Problemen Alerts an die SPECTRUM-Schnittstelle gesendet werden. Lesen Sie die mit dem Produkt bereitgestellte Webhilfe zu Live Exceptions sorgfältig durch, um sicherzustellen, dass Sie das Performance-Konzept verstehen und wissen, wie Performance-Probleme durch Regeln identifiziert werden.

SUCHEN VON LIVE EXCEPTIONS-PROFILEN

Die Live Exceptions-Funktion enthält Hunderte von Standardprofilen, mit denen Sie Ihre Ressourcen überwachen können. Mit Hilfe des Tools „Live Health Profiles“, das auf der Supportsite zur eHealth-Zertifizierung bereitgestellt wird, können Sie die für Ihre Ressourcentypen gültigen Profile suchen und überprüfen.

So überprüfen Sie die verfügbaren Live Exceptions-Profil:

1. Melden Sie sich mit Hilfe eines Webbrowsers auf der Seite <http://support.concord.com> an.
2. Klicken Sie auf „Certification“.
3. Klicken Sie auf der Zertifizierungsseite unter „Certification Information“ auf „Live Health Profile Descriptions“.
4. Klicken Sie auf „Element Types“, um die verschiedenen Ressourcentypen anzuzeigen, die von eHealth überwacht werden können.
5. Blättern Sie in der Elementliste, bis Sie die Ressourcentypen gefunden haben, die Sie momentan überwachen. Wenn Sie z. B. gerade die Aktivitäten der CPUs überwachen, klicken Sie auf „CPU“, „Router/Switch CPU (1)“ und dann auf „Generic Router/Switch CPU (2)“.
6. Klicken Sie auf einen Profilnamen, und lesen Sie die Profilbeschreibung, um herauszufinden, bei welcher Art von Problem ein Alarm ausgelöst wird.

Sie können jedoch auch eigene Profile und Regeln erstellen. Eine Anleitung zum Erstellen eigener Regeln und Profile finden Sie in der Webhilfe zu Live Exceptions.

STARTEN VON LIVE EXCEPTIONS UND ZUGEHÖRIGEN PROFILEN

Zur Verwendung von Live Exceptions müssen Sie sich auf der Weboberfläche von eHealth anmelden und die Live Health-Clientanwendung auf den lokalen PC oder die lokale Workstation herunterladen. Installieren Sie den Live Exceptions-Client entsprechend den Anweisungen auf der Download-Seite.

Um auf die Weboberfläche von eHealth zuzugreifen, navigieren Sie mit Hilfe eines Webbrowsers auf die Seite <http://hostname:port>, wobei *hostname* den Namen oder die IP-Adresse Ihres eHealth-Systems bezeichnet und *port* auf den HTTP-Port des Webserver verweist. Wenn der Webserver den Standardport 80 verwendet, können Sie die Portnummer weglassen. Sie benötigen ein Web User-Konto für eHealth, damit Sie sich auf der Weboberfläche von eHealth anmelden können.

So konfigurieren Sie Live Health, damit bei Problemen ein Alarm ausgelöst wird:

1. Stellen Sie sicher, dass Sie die Live Health-Clientsoftware von der eHealth-Weboberfläche heruntergeladen und installiert haben.
2. Öffnen Sie die Live Exceptions-Anwendung mit einem der folgenden Schritte:
 - > Wenn Sie ein Windows-System verwenden, wählen Sie im Startmenü „Programme“, „eHealth“ und dann „Live Exceptions“. Der Name der Programmgruppe richtet sich nach dem Namen, den Sie bei der Installation des Live Health-Clients verwendet haben.
 - > Wenn Sie ein Unix-System verwenden, wechseln Sie in das Installationsverzeichnis des Live Health-Clients, und führen Sie den Befehl „nhLiveExceptions“ aus.

3. Geben Sie im Feld „eHealth System“ von Live Exceptions den Namen des Systems ein, mit dem Sie eine Verbindung herstellen möchten, und geben Sie dann den Benutzernamen und das Kennwort ein. Der Live Exceptions-Browser wird angezeigt.
4. Wählen Sie „Setup“ und dann „Subjects to Monitor“.
5. Klicken Sie im Dialogfeld „Setup Subjects“ auf „New“.
6. Ordnen Sie im Dialogfeld „Setup Subjects Editor“ der Gruppe oder Gruppenliste ein Profil zu:
 - a. Wählen Sie in der Liste „Subjects“ die Gruppe bzw. Gruppenliste der Elemente aus, die mit Hilfe von Live Health überwacht werden sollen.
 - b. Wählen Sie in der Liste ein geeignetes Profil aus, das dem in der Gruppe bzw. Gruppenliste enthaltenen Elementtyp entspricht.
 - c. Wählen Sie unter „Calendars“ einen Kalender aus, um den Zeitbereich festzulegen, über den Live Health das ausgewählte Profil auf die Gruppe bzw. Gruppenliste anwenden soll.
 - d. Klicken Sie auf „OK“.
 - e. Klicken Sie auf „OK“, um die Eingaben zu bestätigen. Klicken Sie dann im Dialogfeld „Setup Subjects“ auf „OK“. Klicken Sie ein weiteres Mal auf „OK“, um zu bestätigen, dass die Änderungen an den eHealth -Server gesendet wurden.

Live Exceptions beginnt nun mit der Überwachung der Gruppe oder Gruppenliste, um alle Aktivitäten zu identifizieren, die gegen die angegebenen Regeln verstoßen. Wenn eine Aktivität gegen eine im Profil definierte Regel verstößt, löst Live Exceptions einen Alarm aus. Alarme werden i. d. R. mit einer Verzögerung von 15 bis 20 Minuten angezeigt, damit eHealth die Gelegenheit hat, mehrere Anfragen nacheinander an die betreffenden Elemente zu senden.

Weiterleitung von Live Health-Traps an SPECTRUM

Wenn Sie die Traps aus eHealth Live Health an SPECTRUM weiterleiten, können Sie die Live Exceptions-Alarme in der SPECTRUM OneClick-Konsole verwalten, Alarmdetailberichte anzeigen und bei Bedarf Alarme löschen, um die durchschnittliche Reparaturzeit für Netzwerkprobleme zu verringern.

So konfigurieren Sie Live Exceptions für die Weiterleitung von Traps:

1. Starten Sie den Live Exceptions-Browser.
2. Wählen Sie „Setup“ und dann „Trap Destinations“.
3. Klicken Sie im Dialogfeld „Trap Destinations Manager“ auf „New“.
4. Geben Sie unter „Edit Trap Destination“ folgende Informationen zum SpectroSERVER ein:
 - > Hostname
 - > IP-Adresse
 - > Portnummer
5. Klicken Sie auf „Add“.

6. Stellen Sie sicher, dass der Name des SpectroSERVER in der Liste „Existing Trap Destinations“ angezeigt wird, und klicken Sie dann auf „OK“.
7. Wählen Sie „Setup“ und dann „Notifier Rules“.
8. Klicken Sie im Dialogfeld „Notifier Manager“ auf „New“.
9. Führen Sie im Dialogfeld „Notifier Rule Editor“ die folgenden Schritte aus:
 - a. Geben Sie im Namensfeld „SPECTRUM“ ein.
 - b. Wählen Sie in der Aktionsliste den Eintrag „Send Trap“ aus.
 - c. Wählen Sie in der Liste „To NMS“ den SpectroSERVER aus, den Sie in Schritt 4 angegeben haben.
 - d. Wählen Sie unter „When an alarm is“ die Optionen „Raised“ und „Cleared“ aus.
 - e. Geben Sie unter „Elements within“ entweder eine spezielle Technologie an, oder wählen Sie „All Tech/Subjects“.
 - f. Klicken Sie auf „OK“, um die Notifier Rule zu speichern.
10. Überprüfen Sie, ob die Notifier Rule angezeigt wird, und schließen Sie dann das Fenster.

Anpassung und Einplanung von Health-Berichten zur Weiterleitung von Traps

In Health-Berichten wird der allgemeine Zustand einer Gruppe von Elementen bewertet, wobei die aktuelle Performance mit der historischen Performance vergangener Tage, Wochen oder Monate verglichen wird. In dem Bericht werden alle Fehler, auffälligen Auslastungsgrade sowie Schwankungen im Durchsatz protokolliert, die einer weiteren Überprüfung bedürfen.

Die Berichte vermitteln Ihnen einen Überblick über den aktuellen Zustand Ihrer Ressourcen, da überwacht wird, wie effizient diese Ressourcen eingesetzt werden. Darüber hinaus wird überprüft, ob alle kritischen Ressourcen verfügbar sind oder ob bereits erste Probleme in den Ressourcen auftreten. In den Berichten werden auf Basis historischer Daten Trends analysiert und mit Hilfe eines Serviceprofils Durchschnittswerte berechnet.

Sie können die einzelnen Health-Berichte konfigurieren, um die Traps von Health-Exceptions an den SpectroSERVER weiterzuleiten. Wenn ein geplanter Health-Bericht ausgeführt wird, sendet eHealth für das höchstrangige Problem jedes Elements, das im Exceptions-Abschnitt des Health-Berichts angezeigt wird, einen SNMP-Trap an den SpectroSERVER.

Hinweis: Exceptions können nur von geplanten Health-Berichten weitergeleitet werden. Bei der manuellen Ausführung von Health-Berichten werden keine Exceptions weitergeleitet.

So leiten Sie Exceptions aus Health-Berichten weiter:

1. Melden Sie sich bei der eHealth-Konsole an.
2. Wählen Sie „Reports“, „Customize“ und dann „Health Reports“.
3. Wählen Sie den Health-Bericht aus, dessen Ausnahmen Sie weiterleiten möchten.
4. Wählen Sie in der Dropdownliste „Presentation Attributes“ den Eintrag „General“ aus.
5. Wählen Sie in der Attributtabelle die Einträge „NMS IP“ und „Port Trap Address“ aus.
6. Geben Sie im Feld „Value“ die IP-Adresse des SpectroSERVER und die Nummer des SNMP-Ports durch einen Doppelpunkt getrennt ein. Zum Beispiel:

001.02.03.004:162

7. Klicken Sie auf „Apply“, um die Eingaben zu speichern.
8. Wählen Sie in der Dropdownliste „Presentation Attributes“ den Eintrag „Exceptions“ aus.
9. Wählen Sie in der Attributtabelle den Eintrag „Send Exceptions SNMP Trap“ aus.
10. Wählen Sie „Yes“ im Selektionsfeld.
11. Klicken Sie auf „OK“.
12. Klicken Sie auf „Save“, um den benutzerdefinierten Bericht zu speichern.
13. Wählen Sie „Setup“ und dann „Schedule Jobs“.
14. Wählen Sie in der Liste den Eintrag „Add Health Report“ aus.
15. Führen Sie im Dialogfeld „Add Scheduled Report“ die folgenden Schritte aus:
 - a. Wählen Sie den Bericht aus.
 - b. Wählen Sie als Betreff den Technologietyp und die Gruppe aus, die für den Bericht relevant sind.
 - c. Geben Sie für den Bericht einen Zeitbereich und wahlweise eine Zeitzone an.
 - d. Wählen Sie das Format aus, in dem der Bericht ausgegeben werden soll.
 - e. Legen Sie einen Zeitplan für den Job fest.
 - f. Klicken Sie auf „OK“.
16. Klicken Sie auf „OK“.

Konfiguration von eHealth for Voice zum Senden von Alerts an SPECTRUM

Damit SPECTRUM OneClick die von eHealth for Voice beobachteten, sprachspezifischen Probleme in PBXs, Messaging-Systemen und der übrigen Sprachinfrastruktur anzeigen kann, müssen Sie den eHealth for Voice Policy Manager so konfigurieren, dass alle Alerts (SNMP-Traps) an SPECTRUM weitergeleitet werden, wenn eine entsprechende Bedingung eintritt. Zur Konfiguration des Policy Managers müssen Sie eine Richtlinie auf Basis eines definierten Aktionsplans (die Antworten, die den Richtlinien zugeordnet sind) sowie bestimmter Bedingungen erstellen.

So konfigurieren Sie eHealth for Voice, um Alerts an SPECTRUM zu senden:

1. Wählen Sie im Startmenü des Systems, in dem eHealth for Voice installiert ist, „Programme“, „eHealth for Voice“ und dann „eHealth for Voice“. Die Programmkonsole von eHealth for Voice wird angezeigt.
2. Wählen Sie „Tools“ und dann „Service Setup“, um den Policy Manager-Service zu konfigurieren und zu starten.
3. Klicken Sie auf „Configuration“, „Servers to configure the Email“, „SNMP“, „Web“ und dann auf „SPECTRUM servers“.
4. Definieren Sie die Aktionen, die in den Aktionsplan aufgenommen werden sollen:
 - a. Klicken Sie in der Gruppe „Policy Manager“ der Konsolenstruktur auf den Eintrag „Templates“.
 - b. Klicken Sie auf „Actions“.
 - c. Klicken Sie mit der rechten Maustaste in das rechte Fenster, und wählen Sie „New“.
 - d. Geben Sie alle Details zu der Aktionsart ein. Geben Sie auf den Registerkarten „Properties“ und „Configure“ die entsprechenden Informationen ein.
 - e. Klicken Sie auf „Save“.
 - f. Klicken Sie auf „Cancel“, um das Fenster zu schließen.
5. Erstellen Sie eine Aktionsplanvorlage, um die Antworten zu definieren, die der Richtlinie zugeordnet werden sollen:
 - a. Klicken Sie in der Gruppe „Policy Manager“ der Konsolenstruktur auf den Eintrag „Templates“.
 - b. Klicken Sie auf „Action Plans“.
 - c. Klicken Sie mit der rechten Maustaste in das rechte Fenster, und wählen Sie „New“.
 - d. Geben Sie Namen, Beschreibung, Zeitzone und Aktionen an.
 - e. Klicken Sie auf „Save“.

6. Erstellen Sie eine Richtlinie auf Basis des Aktionsplans:
 - a. Klicken Sie in der Gruppe „Policy Manager“ der Konsolenstruktur auf den Eintrag „Policies“.
 - b. Klicken Sie auf „Global“, um eine Richtlinie auf Basis der globalen Daten von eHealth for Voice zu erstellen.
 - c. Klicken Sie mit der rechten Maustaste in den leeren Bereich des rechten Fensters, und wählen Sie im angezeigten Menü den Eintrag „New“.
 - d. Wählen Sie „Blank Policy“, und klicken Sie dann auf „Next“.
 - e. Geben Sie Namen und Beschreibung ein.
7. Klicken Sie auf „Add“.
8. Definieren Sie die Bedingung:
 - a. Geben Sie den Namen, die Plattform des Elements und die Datentabelle an.
 - b. Geben Sie die Kriterien zur Erstellung der Bedingung an.
 - c. Klicken Sie auf „Apply“, um die Bedingung zu speichern.
9. Definieren Sie die Richtlinie:
 - a. Wählen Sie Zeitzone, Betriebsintervall und Zeitrahmen.
 - b. Geben Sie an, wie häufig die Bedingung mit der Richtlinie übereinstimmen muss, bevor der Aktionsplan gestartet wird.
 - c. Geben Sie die Severity an.
 - d. Wählen Sie einen Aktionsplan aus.
 - e. Klicken Sie auf „Save“.

Konfiguration von SPECTRUM zur Erkennung des eHealth-Servers

Nach Abschluss des eHealth-Setups müssen Sie SPECTRUM konfigurieren, damit der eHealth-Server erkannt wird. Auf diese Weise können Sie in der OneClick-Konsole einen Drilldown zu den eHealth-Berichten ausführen und Alarmer löschen.

So aktivieren Sie SPECTRUM zur Erkennung des eHealth-Servers:

1. Melden Sie sich mit Ihren SPECTRUM-Anmeldedaten auf der Homepage von SPECTRUM OneClick an, und klicken Sie auf „Administration“ im oberen Bereich der Seite.
2. Wählen Sie im Menü „Administration“ die Option „eHealth Configuration“.
3. Geben Sie im Konfigurationsfenster von eHealth folgende Informationen ein:
 - > Hostname oder IP-Adresse des eHealth-Servers
 - > Nummer des Ports, über den eHealth Webanfragen empfängt
 - > Benutzername des eHealth-Webadministrators
 - > Kennwort des eHealth-Webadministrators

4. Wählen Sie unter „Alarm Notifier Status“ die Option „Started“, damit die Live Health-Alarme künftig in SPECTRUM gelöscht werden können.

Hinweis: Wenn Sie eHealth und SPECTRUM so konfigurieren, dass die eHealth-Alarme an SPECTRUM weitergeleitet und in SPECTRUM angezeigt werden, können Sie die Alarme mit Hilfe des Alarm Notifiers direkt in der OneClick-Konsole löschen.

5. Klicken Sie auf „Save“.

Konfiguration von SPECTRUM zur Anzeige von eHealth-Alarmen

Nachdem Sie eHealth so konfiguriert haben, dass Live Health-Alarme und -Ausnahmen an einen SpectroSERVER weitergeleitet werden, müssen Sie nun SPECTRUM entsprechend konfigurieren, damit die Alarme dort auch empfangen werden.

So aktivieren Sie SPECTRUM für die Anzeige von eHealth-Alarmen:

1. Melden Sie sich als SPECTRUM-Administrator an.
2. Wählen Sie „Start Console“ im oberen Bereich der OneClick-Seite, um die OneClick-Konsole zu öffnen.
3. Wählen Sie auf der Registerkarte „Explorer“ des OneClick-Navigationsfensters den betreffenden SpectroSERVER aus, und klicken Sie dann auf „Universe“.

Hinweis: Bei Überwachung mehrerer SpectroSERVER wählen Sie den Eintrag „Universe“ für die Umgebung des „Trap Director SpectroSERVER“ aus.

4. Wählen Sie im Fenster „Contents“ die Registerkarte „Topology“.
5. Klicken Sie in der Symbolleiste der Registerkarte „Topology“ auf das Symbol „Create a new model by type“. Das Dialogfeld „Select Model Type“ wird angezeigt.
6. Wählen Sie die Registerkarte „All Model Types“.
7. Wählen Sie „EventAdmin“, und klicken Sie auf „OK“. Das Dialogfeld „Create Model of Type“ wird angezeigt.
8. Geben Sie den Namen und die IP-Adresse des eHealth-Servers an, und klicken Sie auf „OK“. Der eHealth-Server wird in der Topologie als EventAdmin-Modell angezeigt.

Hinweis: Weitere Informationen zur Erstellung von Modellen in OneClick finden Sie im *Modeling Your IT Infrastructure Administrator Guide*.

9. Wählen Sie das EventAdmin-Modell in der OneClick-Topologie aus.
10. Klicken Sie mit der rechten Maustaste auf das EventAdmin-Modell, und wählen Sie „Utilities“ und dann „Attribute Editor“. Das Dialogfeld „Attribute Editor“ wird angezeigt.
11. Wählen Sie in der Attributstruktur den Eintrag „User Defined“, und klicken Sie auf „Add“. Das Dialogfeld „Attribute Selector“ wird angezeigt.
12. Wählen Sie im Fenster „Select Model Type“ die Option „Other“, und wählen Sie dann „EventAdmin“.

13. Wählen Sie im Fenster „Attributes for EventAdmin“ das Attribut „map_traps_to_this_model_using_IP_header“, und klicken Sie auf „OK“. Das Attribut wird in der Liste „User Defined“ des Attribut-Editors angezeigt.
14. Klicken Sie auf den Pfeil, der nach rechts zeigt. Das Attribut wird in das rechte Fenster verschoben.
15. Wählen Sie im rechten Fenster den Eintrag „map_traps_to_this_model_using_IP_header“, und wählen Sie dann „Yes“.
16. Klicken Sie auf „Apply“. SPECTRUM übernimmt die Attribute für das ausgewählte Modell, und das Dialogfeld „Attribute Edit Results“ wird angezeigt.
17. Bestätigen Sie die vorgenommenen Änderungen im Fenster „Attribute Edit Results“, und klicken Sie auf „Close“.
18. Klicken Sie im Attribut-Editor auf „OK“.

Systemwartung

Als Best Practice empfiehlt es sich, die verwendeten eHealth-, OneClick-, SPECTRUM- und eHealth for Voice-Systeme in regelmäßigen Abständen zu sichern. Eine solide Sicherungsstrategie ist dadurch gekennzeichnet, dass Sie das System im Falle eines Datenträgerfehlers, einer Datenbankbeschädigung oder eines anderen unerwarteten Ereignisses umgehend wiederherstellen können. Ohne eine Sicherungsstrategie müssen Sie ggf. Stunden und Tage damit verbringen, die Anwendungen neu zu installieren und zu konfigurieren. Darüber hinaus können Sie dadurch wertvolle Daten verlieren.

Eine vollständige Beschreibung zur Verwaltung der Sicherungskopien Ihrer Systeme und Datenbanken finden Sie in folgenden Handbüchern:

- **SPECTRUM:** *Database Management*
- **eHealth:** *eHealth Database Management Guide*
- **eHealth for Voice:** *eHealth for Voice Operations Guide*

Archive für Systemsicherungen

Mit Hilfe entsprechender Prozeduren können Sie die Sicherungen auf ein Band oder ein anderes System kopieren, das in dem Verzeichnis eines sicheren Benutzers (der lediglich Leserechte besitzt) installiert ist. (Benutzer, die Zugriff auf die gespeicherte Datenbank besitzen, können diese auf einem anderen System wiederherstellen und die darin enthaltenen Daten anzeigen.) Damit die Wiederherstellung hundertprozentig sicher verläuft, sollten Sie die archivierten Daten an einem externen Speicherort aufbewahren. Darüber hinaus sollten Sie über den Erwerb einer Remote-Speicherlösung nachdenken (wie sie z. B. von CA BrightStor angeboten wird), zumal dadurch auch die Verwaltung der Bandbibliotheken entfällt. Sie sollten alle archivierten Sicherungskopien mehrere Monate aufbewahren, damit die Daten und Berichte je nach Bedarf wiederhergestellt werden können. Auf diese Weise können Sie selbst Daten wiederherstellen, deren Beschädigung bereits Monate zurückliegt und bisher noch nicht bemerkt wurde.

Best Practices für die Wiederherstellung von Daten

Als Best Practice empfiehlt es sich, die Daten zunächst probeweise auf einem Testsystem wiederherzustellen, damit Sie sich an die Schritte gewöhnen, bevor tatsächlich ein Problem eintritt.

Kapitel 6: Sammeln der Systeminformationen von Agenten

Systeme stellen wichtige Komponenten des Netzwerks dar. Dort sind i. d. R. alle geschäftskritischen Anwendungen installiert, z. B. Webserver, Datenbanken, E-Mail-Anwendungen und andere für das Unternehmen entscheidenden Anwendungen. Wenn die Systemleistung abfällt, sind die Benutzer nicht mehr in der Lage, ihre Anwendungen auszuführen oder die Aufgaben zu erfüllen, die von diesen Servern unterstützt werden. Dieses Kapitel beschreibt, wie Informationen zur Systemüberwachung gesammelt werden, und stellt Best Practices zur Konfiguration von SPECTRUM und eHealth vor, mit denen die Systemagenten von Unicenter NSM, SystemEDGE und Drittherstellern verwaltet werden können.

Implementation und Administration von Systemagenten

SPECTRUM und eHealth verwenden installierte Systemüberwachungsagenten, um Informationen zu Fehlern und zur Performance zu sammeln. In diesem Kapitel werden drei verschiedene Arten von Systemagenten behandelt:

- die Unicenter NSM-Agenten von CA
- die SystemEDGE-Agenten von CA
- die Agenten von Drittherstellern

Wichtig: Die Installationsschritte für die Unicenter NSM- und SystemEDGE-Agenten werden ausführlich in den produktspezifischen Installationshandbüchern erläutert. **Sie sollten den Anweisungen in den Handbüchern folgen, um die Agenten ordnungsgemäß zu installieren.** Nach Abschluss der Softwareinstallation sollten Sie weiterlesen, um zu erfahren, mit welchen Best Practices Sie SPECTRUM und eHealth konfigurieren können, um diese Agenten effektiv einzusetzen.

Best Practices

Folgen Sie den Anweisungen in den Best Practices, um die Überwachung und Verwaltung der Systemagenten zu vereinfachen:

- Stellen Sie sicher, dass der Systemagent erfolgreich installiert wurde.
- Konfigurieren Sie auf dem System eine SNMP-Community-Zeichenfolge mit Lese- oder Lese-Schreibzugriff.
- Konfigurieren Sie den Systemagenten, um die Traps an den SpectroSERVER weiterzuleiten.
- Stellen Sie sicher, dass Sie die korrekte IP-Adresse und Community-Zeichenfolge eingegeben haben, damit die Agenten erkannt werden.

- Stellen Sie sicher, dass auf den Systemen nur ein Management-Agent aktiviert ist und ausgeführt wird. In einigen Fällen können auf einem System mehrere Agenten ausgeführt werden. Zum Beispiel können der SNMP-Agent von Microsoft und der SystemEDGE-Agent von CA parallel ausgeführt werden. Wenn mehrere Agenten ausgeführt werden und auf SNMP-Anfragen reagieren, können SPECTRUM und eHealth beide Agenten für das gemeinsame System modellieren. Weitere Informationen finden Sie im Abschnitt zu Unicenter NSM-Agenten weiter hinten in diesem Kapitel.

Unterstützte Agenten

In der folgenden Tabelle sind die Unicenter NSM-Agenten aufgeführt, die je nach Version von eHealth und SPECTRUM unterstützt werden. Der Active Directory-Agent and der Performance-Agent werden nur für die Berichterstellung von eHealth unterstützt.

Systemagenten von Unicenter NSM r11	Systemagenten von Unicenter NSM 3.1
UNIX-Systemagenten (caiUxsA2)	UNIX-Systemagenten (caiUxOs)
Windows-Systemagenten (caiWinA3)	Windows-Systemagenten (caiW2kOs)
Agent der Active Directory-Dienste (caiAdsA2)	Agent der Active Directory-Dienste (caiAdsA2)
Log-Agent (caiLogA2)	Log-Agent (caiLogA2)
Performance-Agent (hpxAgent)	Performance-Agent (hpxAgent)

SPECTRUM und eHealth unterstützen alle SystemEDGE-Agenten sowie eine Reihe anderer Agenten, die von Drittherstellern wie Microsoft, Dell, Sun, HP und IBM angeboten werden. Darüber hinaus werden in beiden Anwendungen sämtliche MIB-II- oder RFC 2790-kompatiblen Agenten unterstützt. Beide Anwendungen bieten ein automatisiertes Out-of-box-Fehlermanagement, Trap-Support sowie die Erstellung von Leistungs- und Trendberichten.

Hinweis: Bei Agenten, die die RFC 2790-Erweiterungen von MIB-II unterstützen und verwenden, kann SPECTRUM zusätzlich zur allgemeinen Performance der Hostsysteme auch Prozesse, Dateisysteme und Protokolldateien überwachen. Wenn Agenten ohne die entsprechenden RFC 2790-Erweiterungen erkannt werden, wird ggf. nur die allgemeine Performance der Hostsysteme einschließlich der Protokolldateien überwacht.

Voraussetzungen

Führen Sie zu Beginn folgende Schritte aus:

- Stellen Sie sicher, dass Sie über Administratorberechtigungen verfügen, um auf die SPECTRUM OneClick-Konsole und die eHealth-Konsole zuzugreifen.
- Wenn Sie noch nicht mit der OneClick-Konsole von SPECTRUM gearbeitet haben, finden Sie im *OneClick Administration Guide* alle notwendigen Informationen.
- Wenn Sie noch nicht mit der eHealth-Benutzeroberfläche gearbeitet haben, lesen Sie die Beschreibungen, die im *eHealth Administration Overview Guide* zu eHealth-Konsole und OneClick-Konsole für eHealth (OneClickEH) bereitgestellt werden.

Hinzufügen von Systemagenten in SPECTRUM

Verwenden Sie eine der beiden folgenden Methoden, um die Systemagenten in SPECTRUM hinzuzufügen:

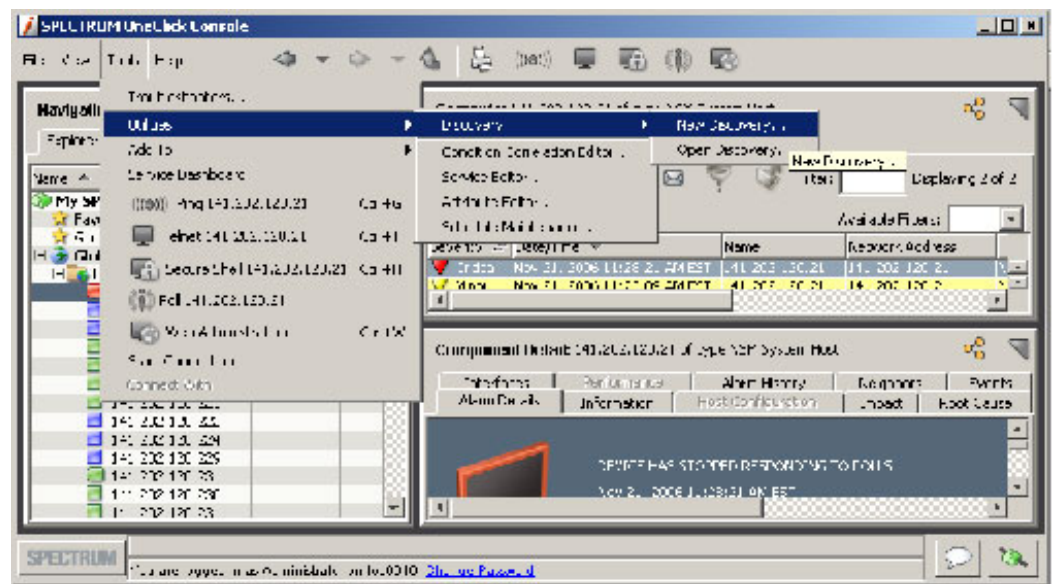
- Führen Sie mit Hilfe der AutoDiscovery-Anwendung von SPECTRUM eine automatische Discovery der Systemagenten durch.
- Fügen Sie die Systemagenten manuell in SPECTRUM hinzu.

AUTOMATISCHE DISCOVERY DER SYSTEMAGENTEN

SPECTRUM verfügt über Funktionen zur automatischen Discovery, mit denen Ihre Systemressourcen automatisch erkannt und modelliert werden können.

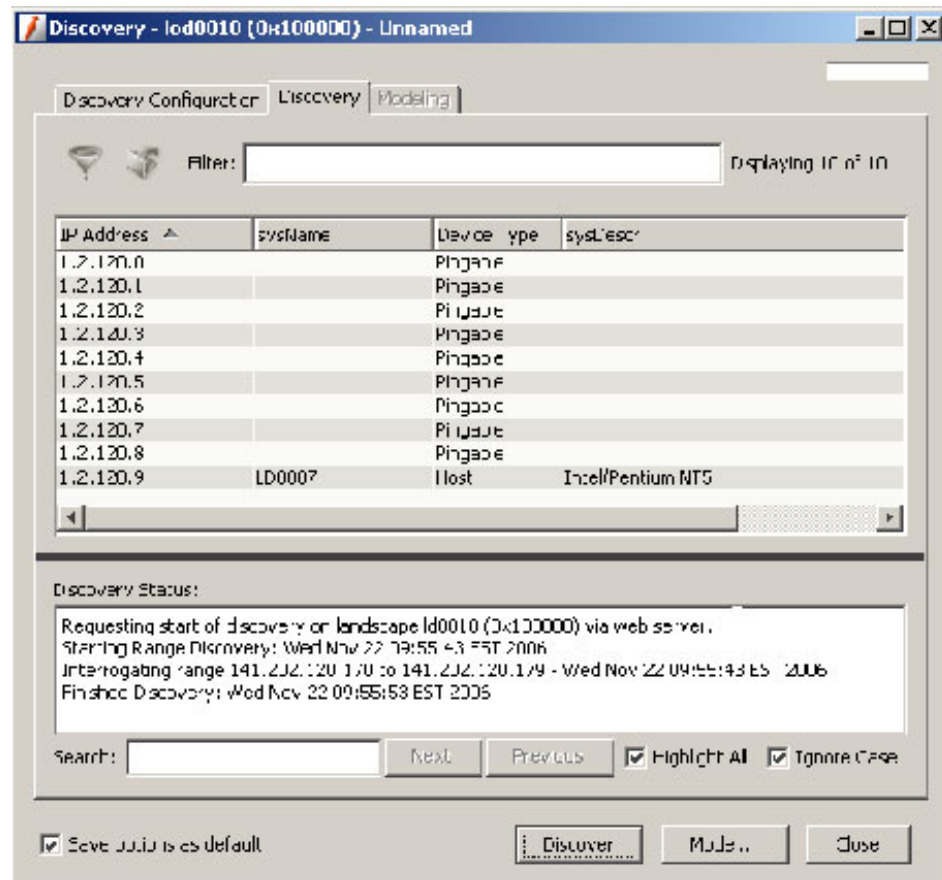
So werden Ihre Systeme automatisch erkannt:

1. Wählen Sie in der SPECTRUM OneClick-Konsole „Tools“, „Utilities“, „Discovery“ und dann „New Discovery“.

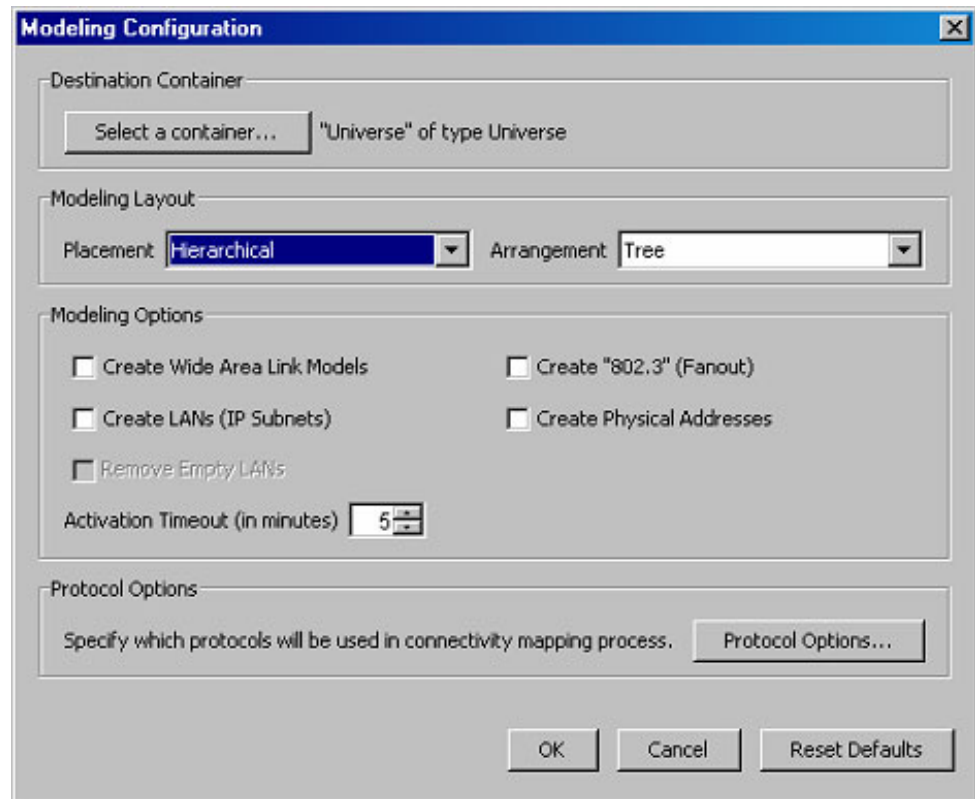


Das Dialogfeld „Discover“ wird angezeigt.

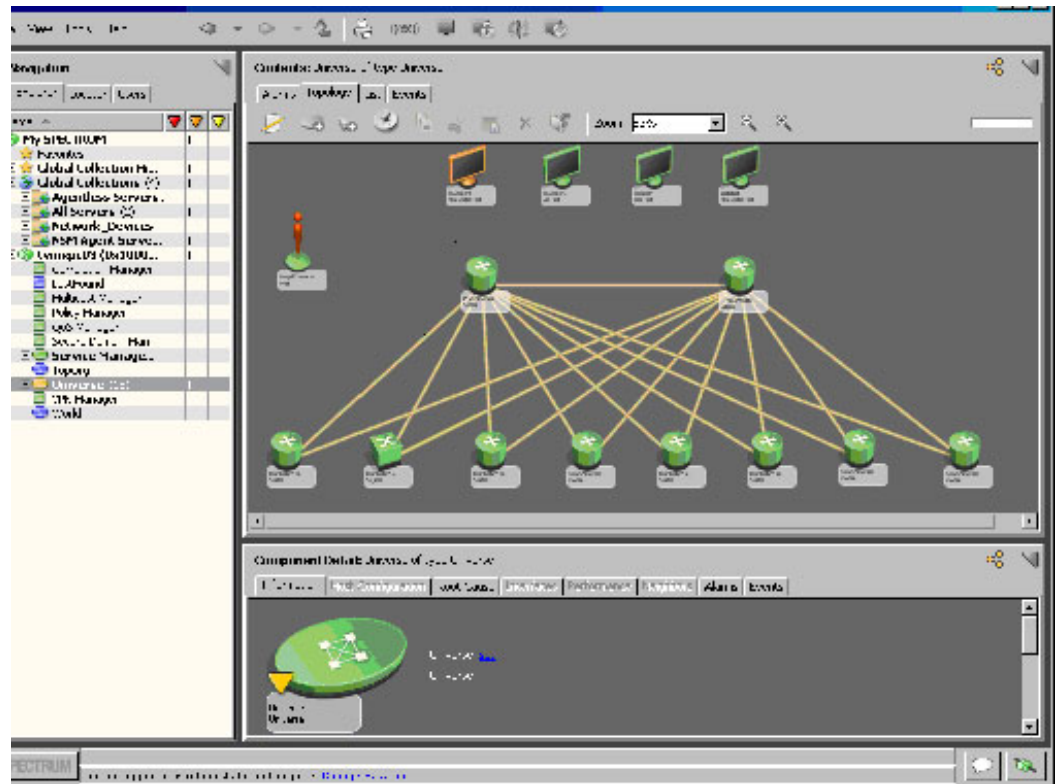
2. Führen Sie im Discovery-Fenster folgende Schritte aus:
 - > Geben Sie einen Konfigurationsnamen an.
 - > Geben Sie einen IP-Bereich oder eine IP-Liste an, oder klicken Sie auf „Import“, um eine Datei mit einer IP-Liste zu importieren.
 - > Geben Sie eine gültige Community-Zeichenfolge an. Wenn Sie mehrere Zeichenfolgen angeben, wird in OneClick zuerst der oberste Eintrag verwendet.
 - > Aktivieren Sie unter „Modeling Options“ die Option „Discover Only“.
 - > Klicken Sie auf „Advanced Options“, und legen Sie Port 6665 fest, um Unicenter NSM-Agenten zu suchen.
3. Klicken Sie auf „Discover“. Das Dialogfeld „Discovery“ wird angezeigt.



4. (Optional) Nachdem die Ergebnisse angezeigt wurden, können Sie Einträge ausschließen, indem Sie mit der rechten Maustaste auf die gewünschten Einträge und dann auf „Exclude“ klicken. Dadurch werden die entsprechenden Geräte in der SPECTRUM-Datenbank nicht „modelliert“.
5. Klicken Sie auf „Model“, um die Systeme zu SPECTRUM hinzuzufügen.



6. Deaktivieren Sie unter „Modeling Options“ die Optionen „Create Wide Area Link Models“ und „Create LANs“. Wenn diese Optionen deaktiviert sind, werden in SPECTRUM nicht automatisch Subnet-Container erstellt. Weitere Informationen zur Discovery und Modellierung finden Sie im *Modeling Your IT Infrastructure Administrator Guide*.
7. Klicken Sie auf „OK“.
8. Klicken Sie im Dialogfeld „Discovery“ auf „Close“, nachdem die Systeme modelliert wurden.



9. (Optional) Klicken Sie in der linken Ecke des Menüs „Tools“ auf das Symbol mit Bleistift und Papier.
10. Sie können die Topologie nach Belieben bearbeiten, indem Sie Symbole verschieben und Hintergrundbilder hinzufügen.

MANUELLES HINZUFÜGEN VON GERÄTEN MIT HILFE VON „CREATE MODEL BY IP ADDRESS“

Als alternative Möglichkeit zur automatischen Discovery der Systeme können Sie diese auch manuell modellieren. Dieser Vorgang kann für Systeme durchgeführt werden, die bei einem Discovery-Prozess nicht antworten.

So modellieren Sie Systemressourcen manuell:

1. Wechseln Sie im OneClick-Navigationsfenster auf der Registerkarte „Explorer“ zu der Topologieansicht „Universe“, in der das neue Gerät angezeigt werden soll. Die ausgewählte Topologieansicht „Universe“ wird auf der Registerkarte „Topology“ des Fensters „Contents“ angezeigt. **Tipp:** Wenn Sie ein neues Gerät in einem Gruppencontainer im Netzwerk positionieren möchten, doppelklicken Sie auf das Containersymbol, um die Topologieansicht für den entsprechenden Container anzuzeigen.
2. Klicken Sie in der Symbolleiste der Registerkarte „Topology“ auf die Schaltfläche „Create model by IP address“. Das Dialogfeld „Create Model by IP Address“ wird angezeigt.



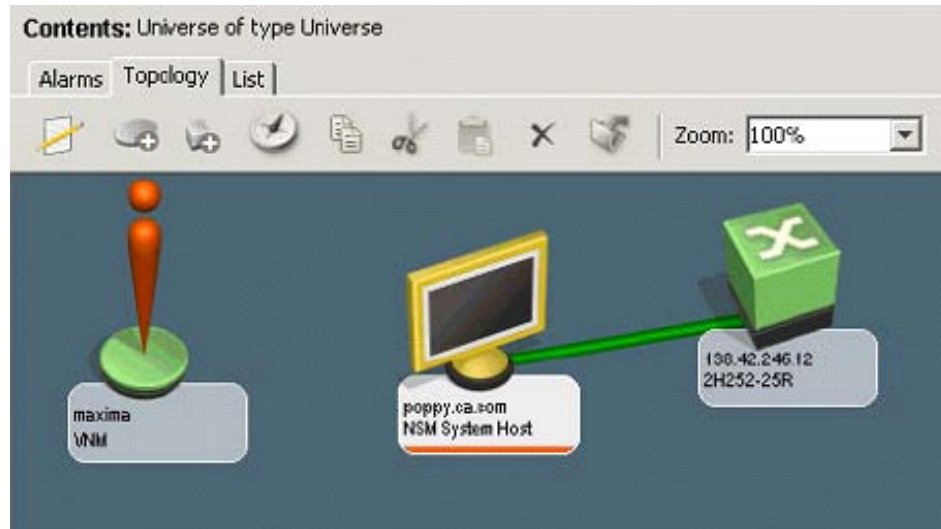
Hinweis: Wenn Sie ein modelliertes Element aus einer Ansicht entfernen möchten, markieren Sie das betreffende Element, und klicken Sie auf *Delete (X)*.

3. Geben Sie die Netzwerkadresse des Geräts an, und nehmen Sie Eingaben in den anderen optionalen Feldern vor, die in der folgenden Tabelle aufgeführt sind.

Einstellungen im Dialogfeld „Create Model by IP Address“

Feld	Beschreibung
Network Address (obligatorisch)	Gibt die Netzwerkadresse (IP-Adresse) des modellierten Geräts an.
Community Name (obligatorisch)	Gibt die SNMP-Community-Zeichenfolge für das zu verwaltende Gerät an.
DCM Timeout (optional)	Gibt den Zeitraum an, in dem Assurance Server auf eine Reaktion des Geräts wartet. Die Standardeinstellung ist 3000 ms.
DCM Retry Count (optional)	Gibt an, wie oft Assurance Server versucht, eine Verbindung mit dem Gerät herzustellen, nachdem das DCM-Zeitlimit abgelaufen ist. Der Standardwert ist 2.
Agent port (optional)	Gibt den Port an, auf dem der Agent SNMP-Anforderungen überwacht. Der Standardport ist 161. (Unicenter NSM-Agenten verwenden Port 6665).
SNMP v2C Enabled (optional)	Gibt an, ob das modellierte Gerät SNMPv2c-Protokolle unterstützt. Aktivieren Sie diese Option, wenn Sie ein Gerät modellieren, das für SNMP v2C konfiguriert ist.
SNMP v3 Enabled (optional)	Gibt an, ob das modellierte Gerät SNMPv3c-Protokolle unterstützt. Aktivieren Sie diese Option, wenn Sie ein Gerät modellieren, das für SNMP v3 konfiguriert ist.
Discover connections (optional)	Ermöglicht, dass in SPECTRUM OneClick die verknüpften Verbindungen (Pipes) zwischen dem (hinzugefügten) Gerät und den benachbarten Geräten erkannt werden.

4. Klicken Sie im Dialogfeld „Create Model by IP Address“ auf „OK“, um ein Gerätesymbol für das angegebene Gerät zu erstellen (oder klicken Sie auf „Cancel“, um den Vorgang abubrechen). Wenn Sie auf „OK“ klicken, wird in SPECTRUM OneClick das neu erstellte Gerätesymbol in der Topologieansicht „Universe“ eingefügt.

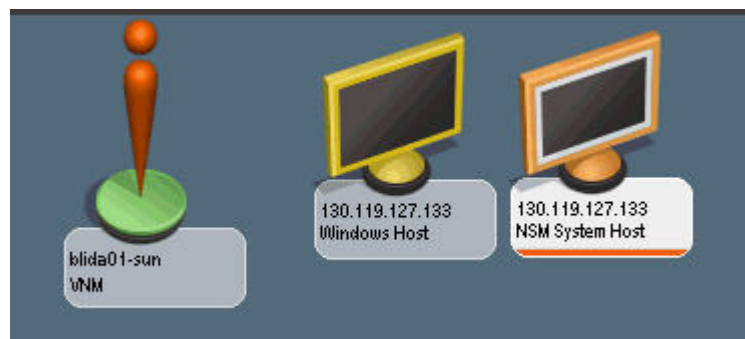


Tipps: Wenn Sie das Symbol eines zuvor modellierten Geräts verschieben oder dessen Darstellung ändern möchten, klicken Sie auf der Symbolleiste der Registerkarte „Topology“ auf die Schaltfläche „Edit“. Sie können die modellierten Geräte folgendermaßen bearbeiten und anordnen:

- Verwenden Sie zum Kopieren oder Einfügen des Symbols eines modellierten Geräts in eine andere Topologieansicht als „Universe“ die Funktionen zum Kopieren und Einfügen auf der Symbolleiste der Registerkarte „Topology“.
- Wenn Sie Konfigurationsparameter (z. B. Community-Name, Abfrageintervall, Anmeldeintervall, Sicherheitszeichenfolge usw.) eines modellierten Geräts ändern möchten, markieren Sie das modellierte Gerät, und ändern Sie die entsprechenden Einstellungen im Fenster „Component Detail“.

Unicenter NSM-Agenten

Sie können Unicenter NSM-Agenten mit Hilfe der SPECTRUM-Discovery automatisch erkennen und modellieren oder diese manuell modellieren. Da Unicenter NSM-Agenten für SNMP-Verbindungen den UDP-Port 6665 und nicht den SNMP-Standardport 161 verwenden, kann SPECTRUM andere auf dem Hostgerät ausgeführte Agenten erkennen und modellieren. Wenn auf einer Windows-Workstation beispielsweise ein Unicenter NSM-Agent, der mit Port 6665 verbunden ist, sowie der Microsoft SNMP-Agent ausgeführt wird, der mit Port 161 verbunden ist, werden in SPECTRUM zwei Modelle für das Gerät erstellt: ein Gerätemodell für den Unicenter NSM-Systemhost und ein Gerätemodell für den Windows-Host, wie in der folgenden Abbildung dargestellt.



Dieses Szenario kann aus den folgenden Gründen zu Leistungsabfällen führen:

- Es werden unnötigerweise doppelte Modelle in SPECTRUM erstellt.
- Dieses Szenario verursacht unnötigen SNMP-Datenverkehr und redundante SNMP-Datenabfragen, was wiederum zu Leistungsabfällen des Netzwerks und von SPECTRUM führen kann.
- Die Leistung des Hostcomputers für den Agenten wird verringert, da mehrere Management-Agenten Performance-Daten bereitstellen.

Führen Sie zum Umgehen dieses Szenarios folgende Schritte aus:

1. Beenden und/oder entfernen Sie vor dem Erkennen und Modellieren alle Management-Agenten mit Ausnahme des Agenten, mit dem das System verwaltet werden soll. Dadurch kann vermieden werden, dass in SPECTRUM mehrere Modelle für den gleichen Host erstellt und verwaltet werden. Achten Sie darauf, bei der Discovery den entsprechenden SNMP-Port festzulegen.
2. Wenn Sie auf einem bestimmten Hostsystem mehrere Agenten ausführen möchten, sollten Sie manuell nur den Agenten modellieren, der mit SPECTRUM verwaltet werden soll.

Hinzufügen von Systemagenten in eHealth

Importieren Sie nach der Discovery und Modellierung von Systemen mit Hilfe von SPECTRUM eine SPECTRUM Global Collection, um die entsprechenden Systemressourcen zur Berichterstellung und Live Health-Überwachung zu eHealth hinzuzufügen. Sie können die Systemressourcen auch mit Hilfe der eHealth-Discovery hinzufügen; für die integrierte Lösung empfiehlt es sich jedoch, die Systeme aus SPECTRUM zu importieren, wie dies in Kapitel 5 beschrieben ist. Nach einigen Abfragezyklen in eHealth können Sie über die OneClick-Benutzeroberfläche Übersichtsberichte und Trend-Berichte ausführen.

Erstellung von Performance-Berichten für Systemagenten

Die gemeinsamen Performance-Daten werden in eHealth für alle verwalteten Systemagenten (Unicenter NSM, SystemEDGE und Agenten von Drittanbietern) vereinheitlicht. Durch die Darstellung aller Performance-Daten in einem gemeinsamen und verständlichen Format minimiert sich die Lernkurve aller Benutzer, die auf Echtzeit- und Verlaufstrendberichte zugreifen.

Übersichtsberichte

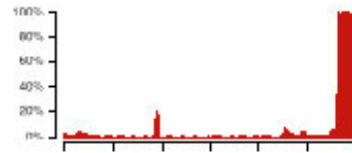
eHealth-Übersichtsberichte für Systemelemente enthalten zusammenfassende Angaben zur Kapazitätsstatistik für das angegebene System, z. B. Prozessor, Interfaces und Partitionsauslastung, Festplattenfehler und E/A sowie Systemverfügbarkeit. Mit Hilfe dieser Berichte können Sie auf schnelle Weise ausgelastete Prozessoren oder volle Festplatten ermitteln sowie Systemgruppen vergleichen. Es folgt ein Beispiel eines Übersichtsberichts für ein Systemelement.

At-a-Glance Report

SysEdge UNIX System Element rainbow-SH

Unix Server

CPU Utilization



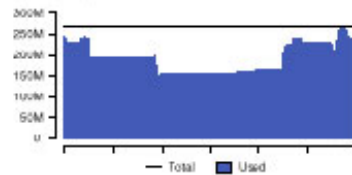
CPU Load Average (processes)



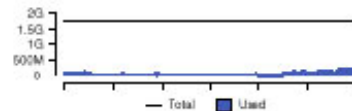
Server Availability



Physical Memory (bytes)



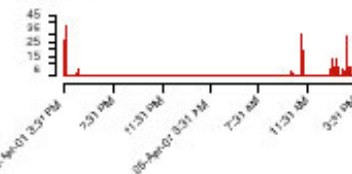
Virtual Memory (bytes)



Page Faults (page faults/sec)

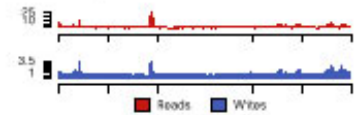


Page Scan Rate (pages/sec)



Time

Disk I/O (reads&writes/sec)



Disk I/O Busy Utilization



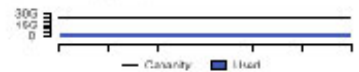
Disk I/O Queue Length (reads&writes)



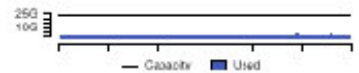
Disk Errors (errors/sec)



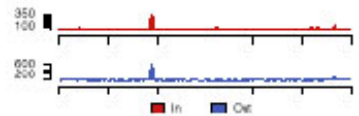
User Partition Space Used (bytes)



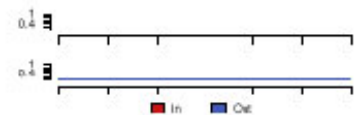
System Partition Space Used (bytes)



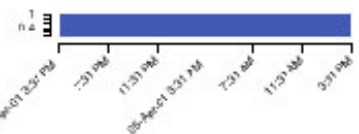
Total Network I/O (frames/sec)



Total Network Errors (errors/sec)



Server Latency (msec)



Time

AUSFÜHREN VON ÜBERSICHTSBERICHTEN

Sie können Übersichtsberichte mit einem der folgenden Verfahren ausführen:

- Klicken Sie in SPECTRUM OneClick mit der rechten Maustaste auf ein Gerät, und klicken Sie dann auf „At-a-Glance Reports“. Der integrierte Übersichtsbericht wird im Hintergrund ausgeführt und automatisch in einem Webbrowser des Systems angezeigt.
- Melden Sie sich über einen Webbrowser auf der eHealth-Weboberfläche mit der URL `http://hostname:port` an. Geben Sie dabei für *hostname* den Namen oder die IP-Adresse Ihres eHealth-Systems und für *port* den vom Webserver verwendeten HTTP-Port an. Wenn der Webserver den Standardport 80 verwendet, können Sie die Portnummer weglassen. Sie müssen über ein eHealth-Webbenutzerkonto verfügen, um sich auf der eHealth-Weboberfläche anmelden zu können. Wechseln Sie zur Registerkarte „Run Reports“, und führen Sie nach Bedarf einen Übersichtsbericht aus.

MyHealth-Berichte für Systeme

Die Seite für einen MyHealth-Bericht der eHealth-Weboberfläche enthält eine Reihe von Diagrammen, die auf Ihre speziellen Anforderungen zugeschnitten sind. Mit MyHealth können Webbenutzer von eHealth mindestens einen benutzerdefinierten Bericht zu kritischen Elementen und Gruppen anzeigen. Eine Seite für einen MyHealth-Bericht umfasst mindestens ein Fenster. In jedem Fenster wird jeweils ein Diagramm angezeigt.

Health-Berichte für Systeme

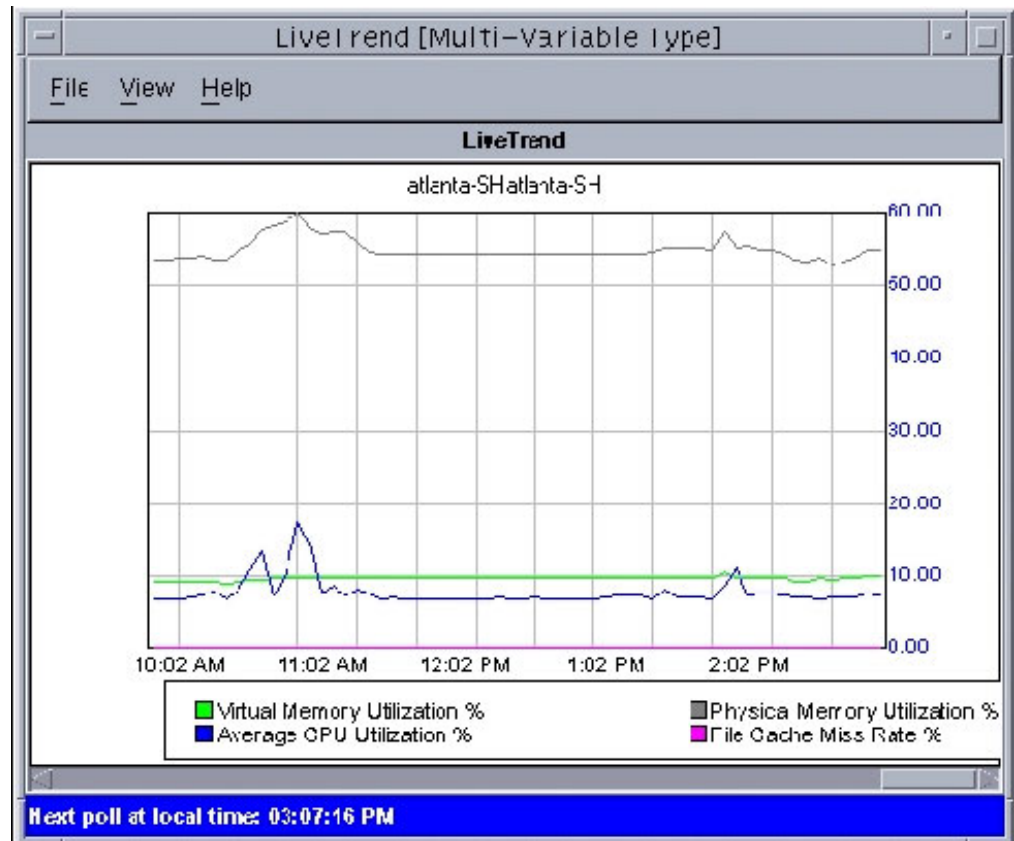
Health-Berichte enthalten Angaben zur Performance einer Gruppe von Elementen im Berichtszeitraum sowie Alerts für Fälle, die Ihrer Aufmerksamkeit bedürfen. Darüber hinaus sind Fälle aufgeführt, die aufgrund von Fehlern, ungewöhnlichen Nutzungsraten oder einer übermäßigen Größe untersucht werden sollten.

Ein Health-Bericht dient folgenden Zwecken:

- Identifizieren von normalem und ungewöhnlichem Systemverhalten
- Vergleichen der Performance einer Gruppe von Elementen in einem Berichtszeitraum mit der Performance in einem Grundzeitraum
- Erkennen von Änderungen im Verhalten, die auf drohende oder bereits vorhandene Probleme hinweisen
- Identifizieren von Kapazitätentrends
- Identifizieren von Systemen, die weiter untersucht werden müssen

Verwendung von Live Trend

Mit Hilfe von Live Trend können Sie Diagramme zur Überwachung statistischer Elemente erstellen, die über eHealth abgefragt werden. Sie können ein einzelnes Diagramm oder mehrere Diagramme in verschiedenen Formaten erstellen, um Elementtrends (einzelnes Element mit mehreren Variablen) oder Variablentrends (einzelne Variable für mehrere Elemente) darzustellen. Im folgenden Live Trend-Diagramm sind vier Variablen in einem System mit der Bezeichnung „atlanta“ dargestellt.



STARTEN VON LIVE TREND

Zur Verwendung von Live Trend müssen Sie sich auf der eHealth-Weboberfläche anmelden und die Live Health-Clientanwendung auf den lokalen Computer oder die lokale Workstation herunterladen. Installieren Sie die Live Health-Clientanwendung entsprechend den Anweisungen auf der Download-Seite. Anschließend können Sie die Live Trend-Anwendung starten und Performance-Echtzeitdiagramme für Ihre Systeme und Ressourcen ausführen.

So starten Sie die Live Trend-Anwendung:

1. Stellen Sie sicher, dass Sie die Live Health-Clientsoftware von der eHealth-Weboberfläche heruntergeladen und installiert haben.
2. Öffnen Sie die Live Trend-Anwendung mit einem der folgenden Schritte:
 - > Wählen Sie in einem Windows-System im Startmenü die Optionen „Programme“, „eHealth“ und dann „Live Trend“ aus. Der Name der Programmgruppe richtet sich nach dem Namen, den Sie bei der Installation des Live Health-Clients verwendet haben.
 - > Wechseln Sie in einem UNIX-System in das Installationsverzeichnis des Live Health-Clients, und führen Sie den Befehl „nhLiveTrend“ aus.
3. Geben Sie im Fenster der Live Trend-Anwendung im Feld „eHealth System“ den Namen des Systems an, mit dem eine Verbindung hergestellt werden soll. Geben Sie anschließend Ihren Benutzernamen und Ihr Kennwort ein. Das Dialogfeld „Live Trend Chart Definition Manager“ wird angezeigt.

Mit Hilfe von Live Trend Chart Definition Editor können Sie benutzerdefinierte Diagramme erstellen und dabei die Elemente und Variablen angeben, deren Daten dargestellt werden sollen. Weitere Informationen finden Sie in der Webhilfe zu Live Trend, die über die eHealth-Weboberfläche aufgerufen werden kann.

Ausführung von Trend-Berichten für Systeme

Anhand von Trend-Berichten können Sie einen oder mehrere Variablenwerte für Ihre Systeme in einem bestimmten Berichtszeitraum ermitteln. Dadurch können Sie die Werte der Variablen nachverfolgen, um den Zeitpunkt zu ermitteln, zu dem sich die Werte möglicherweise grundlegend verändert haben oder zu dem ein bestimmtes Ereignis eingetreten ist, z. B. ein Neustart oder ein Anfragefehler.

Die Trend-Variablen unterscheiden sich je nach Elementtyp. Sie können Berichte für folgende Systeme und Systemkomponenten erstellen:

- Prozessor
- Festplatte
- LAN
- Prozesse und Prozessgruppen
- Benutzer- oder Systempartition
- WAN

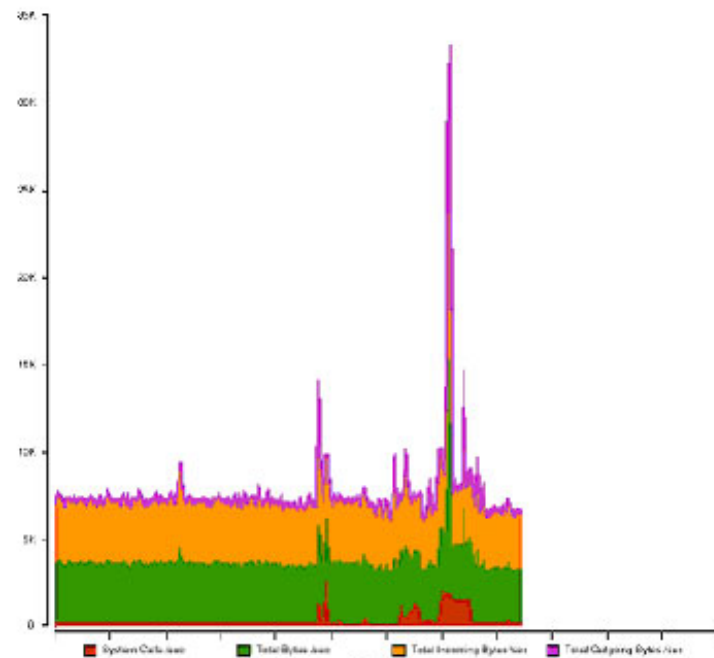
Alle diese Systemtypen oder -komponenten umfassen spezifische Variablen, für die Sie Berichte ausführen können. Serverfestplattenelemente verfügen beispielsweise über Variablen für Lese- und Schreibvorgänge auf der Festplatte sowie für Speicherkapazität und Speichernutzung. Sie können bis zu zehn Variablen gleichzeitig auswählen, für die ein Trend-Bericht ausgeführt werden soll. Eine vollständige Auflistung der Trend-Systemvariablen finden Sie in der Webhilfe zu eHealth.

Im folgenden Beispiel für einen Trend-Bericht sind mehrere häufig vorkommende Systemvariablen abgebildet:

- Total Bytes
- Total Incoming Bytes
- Total Outgoing Bytes
- System Calls

eHealth Trend Report

Divide by Time



Summary Statistics

Sample Time	Delta Time	System Calls /sec	Total Bytes /sec	Total Incoming Bytes/sec	Total Outgoing Bytes/sec
Mean	306	392.74	3.70 K	3.58 K	322.35
Standard Deviation	1	529.81	1.17 K	615.90	602.30
Maximum	306	2.77 K	15.63 K	4.57 K	6.28 K
Minimum	294	107.40	2.96 K	2.72 K	172.49
Size of Range	12	2.66 K	12.67 K	1.85 K	6.09 K
20th Percentile	006	2.69 K	6.56 K	4.65 K	5.12 K
50th Percentile	001	1.09 K	4.88 K	3.69 K	524.19
90th Percentile	001	1.59 K	3.76 K	5.50 K	595.50
Number of samples	206				

From: 04/25/2001 12:09 AM
To: 04/25/2001 11:59 PM

Created: 04/25/2001 04:04 PM

AUSFÜHREN VON TREND-BERICHTEN

Sie können Trend-Berichte über die eHealth-Weboberfläche ausführen.

So erstellen Sie einen Trend-Bericht ähnlich dem obigen Beispiel:

1. Melden Sie sich über einen Webbrowser auf der eHealth-Weboberfläche an.
2. Klicken Sie auf die Registerkarte „Run Reports“.
3. Scrollen Sie im Fensterbereich „Available Reports“ bis zum Bereich für Trend-Berichte.
4. Klicken Sie auf „Standard“.
5. Wählen Sie den Typ „System Element“ aus.
6. Scrollen Sie in der Liste „Elements“, und wählen Sie das gewünschte Systemelement aus.
7. Scrollen Sie in der Liste „Variables“, und wählen Sie Variablen aus. Im Beispielbericht werden die vier folgenden Variablen angezeigt: „Total Bytes“, „Total Incoming Bytes“, „Total Outgoing Bytes“ und „System Calls“.

8. Wählen Sie den Diagrammtyp aus, beispielsweise ein Stapelbalkendiagramm.
9. Scrollen Sie im rechten Fensterbereich, und klicken Sie auf „More Options“.
10. Wählen Sie auf der Registerkarte „General“ die Option „Show Summary Statistics“ aus, damit die Tabellendaten unterhalb des Diagramms angezeigt werden.
11. Klicken Sie auf „Generate Report“. Die Berichtsdaten werden in eHealth verarbeitet. Anschließend wird der Trend-Bericht angezeigt.

Top-N-Berichte

In Top-N-Berichten sind alle Elemente in einer Gruppe aufgeführt, die die angegebenen Berichtsziele über- oder unterschreiten. Sie können zudem ein Ziel für die einzelnen Variablen angeben. In eHealth wird die Differenz zwischen dem tatsächlichen Wert einer Variablen und dem angegebenen Zielwert berechnet.

Konditionale Kapazitätstrend-Berichte für Systeme

Mit Hilfe von konditionalen Kapazitätstrend-Berichten von eHealth können Sie die Kapazitätsplanung durchführen, indem Sie Faktoren für Kapazität und Bedarf solange anpassen, bis die geeignete konditionale Lösung festgelegt ist. Durch die Möglichkeit, potenzielle künftige Szenarios darzustellen, können Sie sich anhand dieser Berichte auf Probleme einstellen, bevor diese auftreten.

Kapitel 7: Service-Level-Management

Im Zentrum der Lösung von CA steht das Konzept der Business Service Intelligence (BSI) - eine Methode zum Verständnis der Beziehungen und der Auswirkungen der IT-Infrastruktur auf Unternehmensservices. BSI bietet Technology Relationship Mapping, Auswirkungsanalyse und Ursachenanalyse. Mit diesen Funktionen können unsere Kunden die Abläufe in ihren IT-Abteilungen von taktisch-reaktiv zu strategisch-proaktiv weiterentwickeln und zugleich die Qualität ihrer IT-Services aus Sicht der Kunden und des Unternehmens verbessern.

Durch die adaptiven Analyseverfahren von BSI werden bidirektionale Verbindungen mit Tausenden von Geräten unterschiedlicher Hersteller und Technologien hergestellt, um komplexe Probleme mit modellbasierten, regelbasierten und richtlinienbasierten Korrelationskomponenten zu identifizieren, zu überprüfen und zu lösen. Die Definition von Unternehmensservices sowie kontinuierliche Wartungsaufgaben werden durch Automatisierung erleichtert. Durch die Planung von Assets, Verfügbarkeit und Kapazitäten, das Änderungsmanagement sowie Leistungs- und Trendanalysen wird die Einhaltung von Service Level Agreements (SLA) validiert. BSI ist ein praktischer, gut umsetzbarer und sich schnell amortisierender Bottom-up-Ansatz für das Business Service Management (BSM).

Die Vorzüge von BSM treten am deutlichsten zutage, wenn die Grunddaten für das Fehler-Management unzulänglich sind und zusätzliche Korrelationen erforderlich sind, um die Auswirkungen zu ermitteln, die möglicherweise aufgrund eines Fehlers entstehen, und die eventuell damit zusammenhängenden Unternehmensservices zu identifizieren. Das Service Management-Modul von SPECTRUM ist mit den Funktionen zum Strukturieren, Analysieren und Steuern aller Aspekte in diesem Bereich ausgestattet. Es umfasst zudem eine Dashboard-Ansicht als Erweiterung von OneClick, in der der Servicezustand direkt in den Mittelpunkt gestellt ist und die komplexe Topologie ausgeblendet wird, die normalerweise in OneClick angezeigt wird.

Im Allgemeinen liegt dem Servicemanagement ein Top-down-Ansatz zugrunde, so dass die Beziehungen und Abhängigkeiten von Geräten, Systemen, Anwendungen und Leistungsmessungen identifiziert werden. In SPECTRUM werden diese als Ressourcen (Modelle oder Daten) und Beziehungen bezeichnet. Diese Ressourcen und Beziehungen werden in Service- oder Subservicemodelle untergliedert. Sie sollten einen Service von unten nach oben definieren, um so die künftige Wiederverwendung häufig verwendeter Services und Subservices zu ermöglichen. Sie können SLAs konfigurieren, um Verstöße dynamisch zu messen und Alerts zu senden.

In diesem Kapitel wird ein Ansatz zum Entwerfen und Implementieren eines Servicemanagement-Systems in der SPECTRUM-Anwendung beschrieben. Im Unterschied zu den meisten Funktionen in SPECTRUM umfasst die Vorbereitung des Servicemanagements möglicherweise eine umfangreiche Planung, damit alle erforderlichen Angaben und Auswirkungen festgelegt werden können.

Die methodische Vorgehensweise in SPECTRUM entwickelt sich mit der Zeit. Wenn bei fortschreitender Implementierung immer mehr Informationen verfügbar werden, bildet sich in der Regel eine detailliertere Darstellung und Einschätzung der Servicemodellierung und des Servicemanagements heraus.

Weitere Referenzquellen:

Service Manager User Guide

Report Manager User Guide

SERVICE Performance Manager User Guide

Interviewverfahren

In diesem Abschnitt wird ein Ansatz zum Entwerfen und Implementieren des Interviewprozesses für das Servicemanagement erörtert.

Interviewfragen

Dokumentieren und erfassen Sie zum Strukturieren und Implementieren des Servicemanagements und Service-Level-Managements die Antworten auf die folgenden Interviewfragen:

- Welche Unternehmensservices möchten Sie überwachen?
- Welche spezifischen Ressourcen unterstützen diese Services?
 - > Prozesse?
 - > Softwareanwendungen?
 - > IT-Geräte?
- Wie können Bedingungen und Fehler, die sich auf Services auswirken, erkannt werden?
- Welche Ressourcenattribute sollen überwacht werden, um den Zustand eines Services zu ermitteln?
- Wer soll bei Fehlern eines angegebenen Services benachrichtigt werden?
- Wie lauten die SLAs, und wie sollen diese quantifiziert werden (Kriterien)?
- Wie ist der kritische Zustand eines angegebenen Services im Verhältnis zu anderen Services oder Subservices definiert?

Allgemeine Fragen

Dokumentieren und erfassen Sie zum Strukturieren und Implementieren des Servicemanagements und Service-Level-Managements die Antworten auf die folgenden allgemeinen Fragen:

- Welche WAN- und LAN-Technologien unterstützen den Service?
- Sind QoS und CoSs derzeit eingerichtet?
- Werden die derzeit verwendeten MPLS-basierten virtuellen privaten Netzwerke (VPNs) überwacht?
- Sind alle kritischen Netzwerkgeräte und -server verwaltbar und werden verwaltet?
- Werden alle Elemente ordnungsgemäß erkannt und entsprechend Ebene 2 oder 3 zugeordnet?
- Sind für die kritischen Interfaces Schwellenwerte konfiguriert?
 - > Fehlerrate?
 - > Löschrage?
 - > Ladevorgänge usw.?

- Müssen Umgebungsfaktoren überwacht werden (Temperatur oder Feuchtigkeit)?
- Müssen Stromnetze oder Netzausfallschutzsysteme überwacht werden?
- Werden die kritischen Protokolldateien oder Windows-Ereignisprotokolle überwacht?
- Werden die kritischen Prozesse oder Windows-Dienste überwacht?
- Werden Anwendungspoints getestet?
 - > File Transfer Protocol (FTP)?
 - > Hypertext Transfer Protocol (HTTP)?
 - > Domänennamensystem (DNS)?
- Wurden für erweiterte Anforderungen benutzerdefinierte Schwellenwerte/Alarmer konfiguriert?
- Kann der Zustand einer Ressource mit Hilfe von Modellattributen ermittelt werden?
- Wurden eindeutige Alarmer mit der Ereignis- oder Bedingungskorrelation erstellt?
- Sind vorhandene oder benutzerdefinierte integrierte Daten mit Alarmdaten aktiviert, die verwendet werden können?
- Wer ist jeweils verantwortlich für den ordnungsgemäßen Betrieb der aufgeführten IT-Ressourcen?
- Können alle Personen auf die korrekten Tools zugreifen, und sind die Kontaktinformationen (E-Mail-Adresse, Telefonnummer usw.) der einzelnen Personen verfügbar?
- Verfügen alle Ressourcen über eine Fehlerbeseitigungsfunktion, oder werden Fehlerbeseitigungsfunktionen zur entsprechenden Benachrichtigung hinzugefügt?
- Welche Benutzer profitieren von den aufgeführten IT-Ressourcen?
- Stufen Sie die einzelnen Benutzer ein:
 - > Sehr gering
 - > Gering
 - > Mittel
 - > Hoch
 - > Sehr hoch
- Wurden für Bestellzwecke logische Benutzergruppen gebildet?
 - > Abteilung
 - > Funktion
 - > Rolle usw.
- Wird der kritische Gerätezustand definiert und/oder für alle Netzwerkgeräte und -server gemessen?

Analyse- und Zuordnungsverfahren

In diesem Abschnitt wird ein Ansatz zum Analysieren und Zuordnen der Ergebnisse aus dem Interviewprozess für das Servicemanagement erläutert.

Gliederung der Informationen zu Ressourcen

Gliedern Sie die für die Services erfassten Informationen mit den folgenden Best Practices.

- Sortieren Sie die Informationen nach geläufigen Informationstypen, beispielsweise:
 - > Anwendungsnamen
 - > Servernamen
 - > Gerätenamen und/oder Gerätetypen
 - > Messkriterien und Quellen dieser Daten
- Legen Sie logische Gruppierungen dieser geläufigen Ressourcen fest, um Duplikate zu vermeiden.

Darstellung der wechselseitigen Beziehungen zwischen Ressourcen

Erstellen Sie ein Diagramm, in dem die Beziehungen zwischen den einzelnen Ressourcen dargestellt sind. Mit Hilfe dieses Diagramms können Sie die wechselseitigen Abhängigkeiten und Auswirkungen der Ressourcen zuordnen.

Segmentierung der Informationen und Zuordnung zu Servicemodellen

Anhand der erfassten und vorbereiteten Informationen können Sie die Servicemodelle erstellen, die mit SPECTRUM überwacht werden sollen.

- Erstellen Sie zunächst entsprechend dem Bottom-up-Ansatz die am häufigsten verwendeten Ressourcenmodelle.
- Legen Sie ein Servicemodell an, indem Sie eine Beziehung zu den entsprechenden Subservicemodellen erstellen.
- Fügen Sie servicespezifische Ressourcen hinzu, die über Subservices nicht verfügbar sind.

Beispiel für die Zuordnung von Unternehmensservices zu Servicemodellen

Kunde XY hat einen kritischen Unternehmensprozess identifiziert. Wenn Kunden von XY telefonisch Aufträge erteilen, geben Bediener diese Aufträge in einem webbasierten System zur Auftragsbearbeitung ein. Die Aufträge werden in einer Oracle-Datenbank gespeichert und verarbeitet. Da während dieses Prozesses viele Probleme auftreten können, möchte Kunde XY einen Service einrichten, der anzeigt, wann die Auftragsbearbeitung beeinträchtigt wird. Im Interviewprozess wurden einige der kritischen Elemente erfasst und dann in der folgenden Hierarchie gruppiert:

- Webserver (WEBORDER1)
 - > Dell-Hardware mit SNMP-Agent (RFC 2790 oder vergleichbar)
 - > Microsoft Internet Information Services (IIS)-Webserver
 - > Protokolldatei mit Einträgen zum kritischen Datenfluss
 - > Überwachung des Prozessors und Speichers erforderlich
 - > Netzausfallschutz durch unterbrechungsfreie Stromversorgung (USV) von APC
 - > Entsprechende Reaktion vom Webserver erforderlich
- Oracle Database Server (WEBDB1)
 - > Dell-Hardware mit SNMP-Agent (RFC 2790 oder vergleichbar)
 - > Oracle Database mit Oracle Intelligent Agent
 - > Überwachung des Prozessors und Speichers erforderlich
 - > Netzausfallschutz durch USV von APC
- Cisco 6509 Catalyst-Switches
 - > DATASW1 zuständig für Verbindungen über den Server
 - > DATASW2 zuständig für Verbindungen über die Bediener-Workstation
- 25 Bediener-Workstations
 - > Überwachung des DNS-Services erforderlich
 - > Funktionalität des DHCP-Services (Dynamic Host Configuration Protocol) erforderlich

Durch Herausarbeiten von Fragen ähnlich den folgenden können Sie den kritischen Zustand von Geräten nach möglichen Fehlern ermitteln:

- Welche katastrophalsten Fehler können eintreten?
- Können alle ausgewählten Elemente gemessen werden?
- Wie ist der kritische Zustand der einzelnen Elemente im Verhältnis zu den anderen Elementen definiert?
- Können Elemente in der Liste wiederverwendet werden oder werden bestimmte Elemente als generische Services für andere IT-Unternehmensprozesse benötigt?
- Mit welchen Prozessen sollen Probleme bearbeitet werden?
- Welcher Fall wäre kritischer: Ausfall von 25 % der Workstations oder Ausfall des Switches, über den eine Verbindung mit den Servern hergestellt wird?

Gruppieren Sie zunächst die kritischsten Ressourcen und die kritischsten Ausfälle. Zweifellos ist der Ausfall der Server oder Switches der katastrophalste mögliche Fehler. Gruppieren Sie daher die Elemente wie folgt:

■ SERVICE: Webbasierte Auftragsbearbeitung

- > Komponenten – WEBORDER1, WEBDB1, DATASW1, DATASW2
 - Wenn eine Komponente ausfällt, fällt der Service aus.
 - Anschlüsse der Switches mit Serververbindungen
 - Wenn ein Anschluss ausfällt, fällt der Service aus.
- > Komponenten – Bediener-Workstations
 - Wenn 75 % der Workstations ausfallen, fällt der Service aus.
 - Wenn 50 % der Workstations ausfallen, verschlechtert sich die Performance des Services.
 - Wenn 25 % der Workstations ausfallen, verschlechtert sich die Performance des Services geringfügig.
- > Performance – Webantwortzeit, TCP-Port für Oracle
 - Wenn beide kritisch sind, fällt der Service aus.
 - Wenn jeweils eine Performance kritisch ist, verschlechtert sich die Performance des Services.
 - Wenn jeweils ein Verstoß vorliegt, verschlechtert sich die Performance des Services geringfügig.
- > Alarmbedingung für alle vier Ressourcen
 - Allgemeiner kritischer Zustand für Alarmbedingungen (geringfügig, schwerwiegend oder kritisch)

Darüber hinaus muss festgestellt werden, wie sich Beeinträchtigungen dieser Unternehmensservices auf Benutzer auswirken. Einfach ausgedrückt: Wer ist davon betroffen, wenn der Unternehmensservice beeinträchtigt ist, und welchen Stellenwert nimmt die betreffende Person ein? Wenn ein Kunde nicht auf die Vertriebswebsite zugreifen kann, stellt dies große Unannehmlichkeiten für ihn dar. Dieser Kunde nimmt daher einen sehr hohen Stellenwert (kritisch) ein.

Wenn interne Benutzer nicht auf einen internen Webserver zugreifen können, der für alltäglich ausgeführte Aufgaben nicht sehr relevant ist, können Sie dieses Problem als geringfügig festlegen. Beantworten Sie die folgenden Fragen, um die Auswirkungen der Unternehmensprozesse besser einstufen zu können:

- Können Sie die aufgeführten Serverbenutzer in der Liste bezüglich ihres Stellenwerts sortieren?
- Können Sie diese Benutzer oder Kunden nach der Sortierung nach Unternehmen, Organisation, Abteilung oder Rolle untergliedern?

Sie sollten zudem die Netzwerkdienste berücksichtigen. Netzwerkdienste wie DNS, DHCP und E-Mail sind zwar allgemeiner, wirken sich jedoch auf die Unternehmensservices aus. Sie können Antwortzeittests einrichten und mit Hilfe eines Services die Server überwachen, die die Dienste bereitstellen. Diese sollten jedoch etwas anders behandelt werden. Da diese Dienste möglicherweise eine gemeinsame Abhängigkeit mit anderen Services aufweisen, sollten Sie bei deren Erstellung die Wiederverwendbarkeit und Modularität berücksichtigen. Es folgt ein Beispiel für einen DNS- und DHCP-Dienst:

■ SUBSERVICE: DNS

- > Komponenten – DNS-Server SERVER-DNS1 und SERVER-DNS2
 - Wenn beide Server ausfallen, fällt der Dienst aus.
 - Wenn nur ein Server ausfällt, verschlechtert sich die Performance des Dienstes geringfügig.
- > Antwortzeittests – Testen der DNS-Antwortzeit
 - Bei Verstößen der Antwortzeit verschlechtert sich die Performance des Dienstes geringfügig.
- > Alarmbedingung für beide Ressourcen
 - Allgemeiner kritischer Zustand für Alarmbedingung (geringfügig, schwerwiegend oder kritisch)

Erstellung von Servicemodellen und Beziehungen

In diesem Abschnitt werden Konzepte und Verfahren der Servicemodellierung eingeführt. Vor dem Erstellen von Servicemodellen sollten Sie sich mit einigen wichtigen Konzepten vertraut machen.

Die wichtigsten Konzepte

- **Ressourcenüberwachung** Bei jedem Servicemodell handelt es sich um eine Ressourcenüberwachung, mit der die zugehörigen Ressourcen aktiv überwacht werden, um so den Zustand der Services zu ermitteln. Servicere Ressourcen sind SPECTRUM-Modelle. Nahezu alle Modelle können als Servicemodelle verwendet werden. Servicere Ressourcen können Gerätemodelle, Interfacemodelle, SPM-Tests, Prozessmodelle und selbst andere Servicemodelle umfassen. Zur Überwachung einer Ressource werden mit dem Service bestimmte Attribute des Ressourcenmodells überwacht. Mit einem Servicemodell können alle Attribute überwacht werden, deren Werte ganze Zahlen sind. Dieses Verhalten eines Services zum Überwachen der Attributwerte der zugehörigen Ressourcen wird als Ressourcenüberwachung bezeichnet.
- **Servicezustand** Der Servicezustand wird durch eine kleine Gruppe von Werten angegeben: aktiv, ausgefallen, verschlechtert und geringfügig verschlechtert. Bei jeder Ressourcenüberwachung wird der zugehörige Servicezustand anhand der Attributwerte der entsprechenden Ressourcen ermittelt. Im Speziellen wird eine Richtlinie für den Servicezustand auf die gemeinsamen Attributwerte aller Ressourcen angewendet. Bei einer Richtlinie handelt es sich im Wesentlichen um eine Formel, mit der ein Wert für den Servicezustand anhand eines oder mehrerer Ressourcenattributwerte berechnet wird. Die mit der Richtlinie angewendete Logik ist in einer Gruppe von Richtlinienregeln eingekapselt. Jede Regel ist eine Anweisung, die bei der Auswertung als „true“ oder „false“ gekennzeichnet wird. Bei der Auswertung einer Richtlinie wird mit der ersten als „true“ gekennzeichneten Regel oder mit der ersten erfüllten Regel der Servicezustand des Services oder der Ressourcenüberwachung ermittelt.

■ **Ursache und Serviceauswirkung** In Anbetracht der Tatsache, dass mit einem Service der zugehörige Zustand durch Überwachen der entsprechenden Ressourcen ermittelt wird, besteht ein logisches wechselseitiges Verhältnis zwischen Ressourcenausfällen und dem Servicezustand. Dieses Verhältnis wird durch Ursache und Serviceauswirkung angegeben. Wenn sich der Zustand eines Services aufgrund des Ausfalls einer Ressource ändert, ist dieser Ausfall die Ursache der Änderung des Servicezustands. Wenn ein Ressourcenausfall den Zustand eines Services beeinflusst, hat der Ausfall gleichermaßen Auswirkungen auf den Service. Diese Konzepte sind von sehr großer Bedeutung für Benutzer, die Serviceausfälle beheben müssen.

■ **Hierarchische Servicemodellierung** Wie weiter oben erwähnt, handelt es sich bei jedem Service um eine Ressourcenüberwachung, mit der der zugehörige Zustand ermittelt wird, indem eine Richtlinie auf eine Gruppe von Attributwerten der entsprechenden Ressourcen angewendet wird. Beachten Sie dabei, dass mit einem Service auch andere Services überwacht werden können. Dadurch können Servicehierarchien erstellt werden. Ein Benutzer kann daher Services mit Komponenten anderer Services erstellen. Dadurch kann die Servicemodellierung wiederum von grundlegenden Services auf niedriger Ebene auf konzeptuelle Servicemodelle auf hoher Ebene erweitert werden.

Erstellung von Servicemodellen

Der Vorgang zum Erstellen eines Servicemodells umfasst die folgenden beiden grundlegenden Schritte:

1. Auswählen von Ressourcen
5. Auswählen der Richtlinie, mit der die Ressourcen überwacht werden

In den folgenden Beispielen wird verdeutlicht, wie ein Benutzer Servicemodelle für webbasierte Services erstellen kann. Weitere Informationen zum Erstellen von Servicemodellen finden Sie im *Service Manager User Guide*.

Beispiel 1: Service für den Zugriff auf Kundenkonten

Die Festlegung der Ressourcen eines bestimmten Services mag Ihnen als äußerst schwieriges Unterfangen erscheinen. In vielen Fällen ist es nicht möglich, dass Sie alle potenziellen Komponenten eines Services in Betracht ziehen und dann zuordnen können, wie sich jede Komponente auf einen bestimmten Service auswirkt. Ein deutlicher Vorteil von SPECTRUM Service Manager liegt darin, dass Sie anfangs kleine, einfache Modelle erstellen und die entsprechende Servicemodellierung in dem Maße fortlaufend verfeinern können, in dem Sie die einzelnen Servicekomponenten besser einordnen und besser einschätzen können, wie sich jede Komponente auf den gesamten Service auswirkt.

Obwohl die Einschätzung aller Komponenten eines Services schwierig ist, ist es in der Regel einfach, einige der wichtigsten Komponenten zu identifizieren, die dann einen effektiven Anfangspunkt bilden. Als Beispiel dient hier ein einfacher Web-Service eines Telefonsupportunternehmens für den Zugriff auf die Daten von Kundenkonten. Dieser Service wird als Service für den Zugriff auf Kundenkonten bezeichnet.

Mit dieser elementaren allgemeinen Beschreibung können Sie bereits einige der Servicekomponenten festlegen. Da es sich um einen webbasierten Service handelt, muss er auf mindestens einem Webserver unterstützt werden. Darüber hinaus bietet der Service Zugriff auf die Daten einer Datenbank mit Kundenkonten. Dies beinhaltet, dass die Datenbank wahrscheinlich auf mindestens einem System ausgeführt wird. In diesem Beispiel wird von einer Umgebung mit zwei Webservern und zwei Datenbankservern ausgegangen. Dies dient als Anfangspunkt zur Modellierung des Services. Wenn beide Webserver oder beide Datenbankserver ausfallen, wird der Service in seiner Gesamtheit nicht ausgeführt. Solange ein Webserver und ein Datenbankserver aktiv sind, wird der Service ausgeführt, dennoch ist wahrscheinlich eine Leistungsver schlechterung zu verzeichnen. Diese sehr einfache Beschreibung bildet die Grundlage zum Erstellen des Services für den Zugriff auf Kundenkonten.

- Legen Sie bei der anfänglichen Gerätemodellierung in SPECTRUM jeden Webserver und Datenbankhost als Ressourcenmodell fest. Bei der Überwachung des Verbindungsstatus dieser Gerätemodelle wird festgestellt, ob die Systeme aktiv sind. Wie im Abschnitt „Die wichtigsten Konzepte“ erläutert, handelt es sich bei jedem Service um eine Ressourcenüberwachung.
- SPECTRUM umfasst eine Grundformel für den Servicezustand, die eine allgemeine Einschätzung der Verfügbarkeit dieser vier Ressourcen des Services ermöglicht. In der folgenden Tabelle ist eine Matrix dargestellt, in der jede Komponente sowie die Auswirkungen des entsprechenden Status (aktiv/ausgefallen) auf den Service relativ zum Status der anderen Ressourcen aufgeführt sind.

Matrixtabelle für den Servicezustand

Webserver 1	Webserver 2	Datenbankserver 1	Datenbankserver 2	Service
VERBUNDEN	VERBUNDEN	VERBUNDEN	VERBUNDEN	AKTIV
UNTERBROCHEN	VERBUNDEN	VERBUNDEN	VERBUNDEN	GERINGFÜGIG VERSCHLECHTERT
VERBUNDEN	UNTERBROCHEN	VERBUNDEN	VERBUNDEN	GERINGFÜGIG VERSCHLECHTERT
VERBUNDEN	VERBUNDEN	UNTERBROCHEN	VERBUNDEN	GERINGFÜGIG VERSCHLECHTERT
VERBUNDEN	VERBUNDEN	VERBUNDEN	UNTERBROCHEN	GERINGFÜGIG VERSCHLECHTERT
UNTERBROCHEN	VERBUNDEN	UNTERBROCHEN	VERBUNDEN	VERSCHLECHTERT
UNTERBROCHEN	VERBUNDEN	VERBUNDEN	UNTERBROCHEN	VERSCHLECHTERT
VERBUNDEN	UNTERBROCHEN	UNTERBROCHEN	VERBUNDEN	VERSCHLECHTERT
VERBUNDEN	UNTERBROCHEN	VERBUNDEN	UNTERBROCHEN	VERSCHLECHTERT
UNTERBROCHEN	UNTERBROCHEN	VERBUNDEN	VERBUNDEN	AUSGEFALLEN
UNTERBROCHEN	VERBUNDEN	UNTERBROCHEN	UNTERBROCHEN	AUSGEFALLEN
VERBUNDEN	UNTERBROCHEN	UNTERBROCHEN	UNTERBROCHEN	AUSGEFALLEN
VERBUNDEN	VERBUNDEN	UNTERBROCHEN	UNTERBROCHEN	AUSGEFALLEN
UNTERBROCHEN	UNTERBROCHEN	UNTERBROCHEN	UNTERBROCHEN	AUSGEFALLEN

Die Tabelle zeigt, dass der Service ausfällt, wenn beide Webserver oder beide Datenbankserver ausfallen. Wenn ein Webserver und ein Datenbankserver ausfallen, verschlechtert sich der Service. Wenn einer der Server ausfällt, verschlechtert sich der Service geringfügig. Hierbei handelt es sich um einen sehr vereinfachten Ansatz, der jedoch eine gute Ausgangsbasis bildet.

Auf der Grundlage dieses Ansatzes können Sie festlegen, wie die einzelnen Komponenten überwacht werden sollen. In der Tabelle ist dargestellt, dass bestimmte Kombinationen der Statuswerte zu einem spezifischen Verschlechterungsgrad des Services führen. Im Wesentlichen können Sie die Ressourcen in Webserverkomponenten und Datenbankkomponenten unterteilen und sich die gruppierten Ressourcen als Services innerhalb eines Services vorstellen. Damit der Service für den Zugriff auf Kundenkonten ausgeführt werden kann, müssen die Webserverkomponenten und die Datenbankkomponenten ausgeführt werden. Der Service für den Zugriff auf Kundenkonten kann kleine, speziellere Subservices umfassen.

Da es sich bei jedem Service auch um eine Ressourcenüberwachung handelt, eignet sich dieses Beispiel gut zum Erstellen einer Ressourcenüberwachung innerhalb des Services für den Zugriff auf Kundenkonten (siehe folgende Abbildung).



Mit der Ressourcenüberwachung können Sie Ressourcen gliedern und anhand spezifischer Kriterien hinsichtlich der jeweiligen Auswirkungen auf den Service überwachen. Mittels der Ressourcenüberwachung werden mehrere Ressourcen abstrahiert. Zudem wird auf der Grundlage des gemeinsamen Status der überwachten Ressourcen ein Zustandswert ausgegeben. Dieser dient als Basis für eine Richtlinie zum Überwachen der Servicere Ressourcen.

In diesem Beispiel wurde festgesetzt, dass der Verbindungsstatus der einzelnen Gerätemodelle überwacht werden kann, um die jeweilige Verfügbarkeit zu ermitteln. Zusätzlich ist in der Tabelle angegeben, wie sich verschiedene Kombinationen aus Verbindungsstatuswerten auf den Service auswirken. Für die Webserver kann zunächst eine Richtlinie festgelegt werden, mit der der Gesamtstatus der einzelnen Webserverkomponenten ermittelt wird. Diese Anweisungen können als Richtlinie für Webserverredundanz bezeichnet werden.

RICHTLINIE FÜR WEBSERVERREDUNDANZ

- Wenn die Verbindung mit allen Webservern unterbrochen ist, fällt die Webserverkomponente des Services aus.
- Wenn die Verbindung mit einem Webserver unterbrochen ist, verschlechtert sich die Leistung der Webserverkomponente des Services.

Die Webkomponenten und Datenbankkomponenten werden als Services in einem Service beschrieben. Dieses Konzept ist wichtig, wenn Ressourcengruppen verarbeitet werden, die einen bestimmten Aspekt eines Services unterstützen. In allen Fällen fällt der Service für den Zugriff auf Kundenkonten aus, wenn beide Webserver ausfallen. Wenn nur ein Webserver ausfällt, muss dies jedoch nicht zwangsläufig bedeuten, dass der Service für den Zugriff auf Kundenkonten ausfällt oder sich dessen Leistung verschlechtert. Sie können sich die Webserver in ihrer Gesamtheit als Komponente des Services vorstellen. Wenn einer der Server ausfällt, verschlechtert sich diese Komponente des Services. Dies mag noch nicht ganz einleuchtend erscheinen, mit der Weiterentwicklung des Servicemodells wird jedoch klar, warum dieser Ansatz gewählt werden sollte.

Die Auswirkungen des Ausfalls der Datenbankserver entsprechen denen hinsichtlich des Ausfalls der Webserver. Diese Anweisungen können als Richtlinie für Datenbankserverredundanz bezeichnet werden.

RICHTLINIE FÜR DATENBANKSERVERREDUNDANZ

- Wenn die Verbindung mit allen Datenbankservern unterbrochen ist, fällt die Datenbankkomponente des Services aus.
- Wenn die Verbindung mit einem Datenbankserver unterbrochen ist, verschlechtert sich die Leistung der Datenbankkomponente des Services.

Die Webserver und die Datenbankserver wurden in ihrer Gesamtheit als Webserverkomponente und Datenbankkomponente beschrieben. Ziehen Sie in Erwägung, wie sich die Webserverkomponente und die Datenbankkomponente auf den Service für den Zugriff auf Kundenkonten auswirken.

Wenn beide Webserver — oder beide Datenbankserver — ausfallen, fällt der Service aus. Die Server wurden in zwei Gruppen unterteilt: eine Webserverkomponente und eine Datenbankkomponente. Diese können als Ressourcenüberwachung für Webserver und als Ressourcenüberwachung für Datenbankserver bezeichnet werden. Mit jeder Ressourcenüberwachung wird anhand der jeweils überwachten Ressourcen der entsprechende Zustandswert ermittelt. Mit der Ressourcenüberwachung für Webserver wird der Zustand anhand des Verbindungsstatus von Webserver 1 und Webserver 2 ermittelt. Mit der Ressourcenüberwachung für Datenbankserver wird der Zustand anhand des Verbindungsstatus von Datenbankserver 1 und Datenbankserver 2 ermittelt.

Durch Kapselung der Webserver und der Datenbankserver in die Ressourcenüberwachung werden diese Anweisungen berücksichtigt, die als Standardrichtlinie für den Kontenzugriff bezeichnet werden.

STANDARDRICHTLINIE FÜR DEN KONTEZUGRIFF

- Wenn eine Ressourcenüberwachung ausfällt, fällt der Service für den Zugriff auf Kundenkonten aus.
- Wenn sich die Leistung der gesamten Ressourcenüberwachung verschlechtert, verschlechtert sich der Service für den Zugriff auf Kundenkonten.
- Wenn sich die Leistung einer Ressourcenüberwachung verschlechtert, verschlechtert sich die Leistung des Services für den Zugriff auf Kundenkonten geringfügig.

Obwohl in jeder Ressourcenüberwachung Redundanzen auftreten, fällt der gesamte Service aus, wenn eine Ressourcenüberwachung ausfällt. Dieser Entwurf kann im Hinblick auf die Tabelle mit den Werten für Verbindungsstatus und Servicezustand validiert werden. Sie können den Entwurf mit den folgenden drei Szenarien testen.

ENTWURF DER TESTSZENARIEN

- Webserver 1 ist ausgefallen. Dadurch verschlechtert sich die Leistung der Ressourcenüberwachung für Webserver. Dies wirkt sich nicht auf die Datenbankserver aus, da die Ressourcenüberwachung für Datenbankserver aktiv ist. Anwendung der in der Richtlinie für den Kontenzugriff definierten Regeln:
 - > Die erste Regel ist nicht erfüllt, da keine Ressourcenüberwachung ausgefallen ist.
 - > Die zweite Regel ist nicht erfüllt, da die Ressourcenüberwachung für Datenbankserver aktiv ist und die Leistung sich nicht verschlechtert hat.
 - > Die dritte Regel ist jedoch erfüllt, da sich die Leistung der Ressourcenüberwachung für Webserver verschlechtert hat.

In diesem Szenario wird eine geringfügige Verschlechterung des Services für den Zugriff auf Kundenkonten verzeichnet. Entsprechend den Angaben in der Matrix verschlechtert sich der Gesamtzustand des Services geringfügig, wenn Webserver 1 ausgefallen ist und alle anderen Geräte aktiv sind. Der Entwurf kann für dieses Szenario verwendet werden.

- Webserver 1 und Datenbankserver 1 sind ausgefallen. Auf der Grundlage der oben beschriebenen Implementierung führt dies zu einer Verschlechterung der Ressourcenüberwachung für Webserver und der Ressourcenüberwachung für Datenbankserver. Die Auswertung der Richtlinie für den Kontenzugriff ergibt, dass die zweite Regel erfüllt ist und sich der Service für den Zugriff auf Kundenkonten verschlechtert. Entsprechend den Angaben in der Matrix verschlechtert sich der Gesamtzustand des Services, wenn Webserver 1 und Datenbankserver 1 ausgefallen sind. Auch dieser Entwurf funktioniert ordnungsgemäß.
- Datenbankserver 1 und Datenbankserver 2 sind ausgefallen. In diesem Fall fällt die Ressourcenüberwachung für Datenbankserver aus. Bei der Überprüfung der Richtlinie für den Kontenzugriff ergibt sich, dass die erste Regel erfüllt ist. Dies führt zu einem Ausfall. Entsprechend den Angaben in der Matrix fällt der gesamte Service aus, wenn Datenbankserver 1 und 2 ausfallen.

Obwohl es sich um ein sehr einfaches Beispiel handelt, wurden bei diesem Vorgang die Ressourcen eines Services sowie die Art ihrer Überwachung ermittelt. Trotz ihrer Einfachheit umfasst diese Implementierung Angaben zur korrekten Meldung des Zustands des Services für den Zugriff auf Kundenkonten für dreizehn verschiedene Fehlerszenarien, einschließlich der Hostsysteme für die Webserver- und Datenbankserver-Anwendungen. Diese Implementierung ist offensichtlich noch nicht sehr stabil, da die vier Systeme nur daraufhin geprüft werden, ob sie aktiv oder ausgefallen sind. Führen Sie vor dem Erweitern des Services für den Zugriff auf Kundenkonten die folgenden Schritte aus, um den Entwurf mit Hilfe von SPECTRUM Service Manager zu implementieren.

IMPLEMENTIERUNG VON BEISPIEL 1 IN SPECTRUM

In SPECTRUM können Sie Servicemodelle über den Service Editor erstellen, den Sie in der OneClick-Konsole im Menü „Tools“ unter „Utilities“ starten können.

So erstellen Sie ein Servicemodell:

1. Wählen Sie in der OneClick-Konsole die Optionen „Tools“, „Utilities“ und dann „Service Editor“ aus.
2. Klicken Sie auf „Create“.
3. Geben Sie den Richtliniennamen „Verbindungsüberwachung für Webserver“ sowie eine Beschreibung und eine Sicherheitszeichenfolge an.
4. Klicken Sie auf die Schaltfläche zum Suchen von Ressourcen und Containern (Fernglassymbol).
5. Klicken Sie im linken Fensterbereich des Dialogfelds „Locate Resources“ auf „Devices“, „Devices“, „By Model Name“ (oder „By IP Address“). Suchen Sie die ausgewählten Geräte (Fernglassymbol). Geben Sie Suchkriterien an (vorangestellte und nachgestellte Wildcards implizieren den Namen des Modells), und klicken Sie auf „OK“.
6. Wählen Sie im rechten Fensterbereich alle Servermodelle aus, die dem Servicemodell zugeordnet werden sollen.
7. Klicken Sie auf „Add Selected to Monitored Resources“.
8. Klicken Sie auf „Close“.

9. Klicken Sie auf „Select“, um das Dialogfeld „Select Policy“ zu öffnen. Bei der Ressourcenüberwachung wird die Richtlinie für Webserverredundanz verwendet, die weiter oben in diesem Kapitel beschrieben wurde.
10. Wählen Sie im linken Fensterbereich „Contact Status“ als „Value Map“ aus.
11. Klicken Sie auf „New“ im Regelsatz, und geben Sie den Namen „Regeln für Webserverredundanz“ für den Regelsatz ein.
12. Klicken Sie auf „Add“, und erstellen Sie dann die erste Regel „Rule Type All, When all are Down, the service is Down“.
13. Klicken Sie auf „OK“.
14. Klicken Sie auf „Add“, und erstellen Sie dann die zweite Regel „Rule Type Any, When any 1 are Down, the service is Degraded“.
15. Klicken Sie auf „OK“.
16. Klicken Sie im Dialogfeld „Create Rule Set“ auf „Create“.
17. Klicken Sie auf „OK“.
18. Klicken Sie im Dialogfeld „Create Service“ auf „Create“.
19. Wiederholen Sie die Schritte 2 bis 10, um die Richtlinie „Verbindungsüberwachung für Datenbankserver“ zu erstellen.

Hinweis: Diese Richtlinie ist mit „Regeln für Webserverredundanz“ identisch.

20. Wählen Sie im rechten Fensterbereich „Regeln für Webserverredundanz“ aus, und klicken Sie auf „Copy“.
21. Legen Sie den Namen „Regeln für Datenbankserverredundanz“ für den neuen Regelsatz fest.
22. Klicken Sie auf „Create“.
23. Klicken Sie auf „OK“, um das Dialogfeld „Select Policy“ zu schließen.
24. Klicken Sie im Dialogfeld „Create Service“ auf „Create“.
25. Klicken Sie auf „Create“, um in der hierarchischen Struktur den Service auf oberster Ebene (Service für den Zugriff auf Kundenkonten) zu erstellen.
26. Geben Sie den Servicenamen „Service für den Zugriff auf Kundenkonten“ und optional eine Beschreibung und eine Sicherheitszeichenfolge an.
27. Klicken Sie auf das Fernglassymbol und anschließend auf „Locater“, „Services“, „Services“, „All“. Starten Sie die gewünschte Suche (Fernglassymbol).
28. Wählen Sie „Landscape“ aus, wenn diese Option angezeigt wird.
29. Wählen Sie die Services „Verbindungsüberwachung für Webserver“ und „Verbindungsüberwachung für Datenbankserver“ aus.

30. Klicken Sie auf „Add Selected to Monitored Resources“.
31. Klicken Sie auf „Close“.
32. Klicken Sie auf „Select“, um das Dialogfeld „Select Policy“ zu öffnen.
33. Wählen Sie im linken Fensterbereich „Service Health“ als „Value Map“ aus.
34. Klicken Sie auf „New in the Rule Set“, und geben Sie den Namen „Standardrichtlinie für den Kontenzugriff“ für den Regelsatz ein, der auf folgenden Regeln beruht:
 - > Rule Type Any: When any 1 are Down, the service is Down.
 - > Rule Type All: When all are Degraded, the service Degraded.
 - > Rule Type Any: When any 1 are Degraded, the service is Slightly Degraded.
35. Klicken Sie im Dialogfeld „Rule Set“ auf „Create“.
36. Klicken Sie auf „OK“.
37. Klicken Sie im Dialogfeld „Create Service“ auf „Create“.
38. Schließen Sie das Fenster.

ÜBERBLICK BEISPIEL 1

Der Entwurf für Beispiel 1 umfasst einen Service mit zwei Ressourcenüberwachungen. Es handelt sich um einen zweistufigen Ansatz, bei dem mit jeder Ressourcenüberwachung der Status der jeweils entsprechenden Ressourcen konsolidiert und anschließend das Ergebnis als jeweils zugehöriger Servicezustand verzeichnet wird. Mit dem Service für den Zugriff auf Kundenkonten wird dann der zugehörige Servicezustand anhand der kombinierten Servicezustände der beiden Ressourcenüberwachungen ermittelt. Dieses wichtige abstrakte Muster ist von großer Bedeutung für das Verständnis des Servicemanagements.

Mit jeder Service- und Ressourcenüberwachung werden zwei Aufgaben durchgeführt:

- Überwachen der jeweils zugeordneten „Ressourcen“
- Ermitteln des entsprechenden Servicezustands durch Anwenden der Werte dieser Ressourcen auf eine Richtlinie

Berücksichtigen Sie bei der Implementierung von Beispiel 1 folgende Fragen:

- Wird Datenbankserver 2 mit dem Service für den Zugriff auf Kundenkonten ermittelt?

In den drei Testszenarien wird nicht erwähnt, dass Datenbankserver 2 mit dem Service für den Zugriff auf Kundenkonten überwacht wird. In Szenario 3 wurde jedoch für den Fall, dass Server 1 und 2 ausfallen, mit dem Service für den Zugriff auf Kundenkonten folgerichtig ermittelt, dass der Service ausfällt.

■ Wie wurde dies ermittelt?

Mit der Ressourcenüberwachung für Datenbankserver wurde ermittelt, dass der zugehörige Zustand „Ausgefallen“ lautet. Mit dem Service für den Zugriff auf Kundenkonten, mit dem die Ressourcenüberwachung für Webserver und die Ressourcenüberwachung für Datenbankserver überwacht werden, wurde ermittelt, dass der Zugriffsservice auch ausfällt. Beim Auswerten der zugehörigen Richtlinie für den Kontenzugriff wurde festgestellt, dass eine Ressourcenüberwachung ausgefallen ist und daher der Service auch ausfällt. Die Datenbankserver 1 und 2 sind „Ressourcen“ der Ressourcenüberwachung für Datenbankserver, die Ressourcenüberwachung für Datenbankserver ist wiederum eine „Ressource“ des Services für den Zugriff auf Kundenkonten. Jede Komponente ermittelt den zugehörigen Zustand anhand der entsprechenden Ressourcen.

Beispiel 2: Erweiterung des Services zur Überwachung kritischer Prozesse

In Beispiel 1 wird beschrieben, wie ein sehr einfacher Service mit zwei Ressourcenüberwachungen entworfen und implementiert wird. Obwohl dies ein vertretbarer Service ist, handelt es sich um keinen vollständigen Service. Der Service für den Zugriff auf Kundenkonten kann im Hinblick auf die Überwachung der Servicekomponenten auf verschiedene Weise erweitert werden. Bis jetzt wird im Service lediglich der Verbindungsstatus der Geräte berücksichtigt, auf denen die Webserver und die Datenbankserver ausgeführt werden. Mit der Geräteverfügbarkeit allein wird jedoch nicht sichergestellt, dass Sie Kundendaten abrufen können.

Sie müssen darüber hinaus in Betracht ziehen, dass es sich bei einem Webserver um eine Anwendung handelt, mit der Webtransaktionen unterstützt werden. Diese Anwendung muss ausgeführt werden, damit Zugriffsanforderungen auf Kundenkonten verarbeitet werden können. In Anbetracht des kritischen Zustands dieser Webserverssysteme ist es nur logisch, dass diese auch Agenten zur Unterstützung der Prozessüberwachung oder MIB-Informationen, wie sie beispielsweise durch RFC 2790 definiert sind, unterstützen. Dadurch können Benutzer den eigentlichen Webserverprozess überwachen.

Sie können mit einem Prozessmodell ermitteln, ob ein bestimmter Prozess tatsächlich auf einem Gerät durchgeführt wird. Für den Fall, dass das Webserverssystem aktiv ist, die Webserveranwendung jedoch nicht ausgeführt wird, ist die zusätzliche Überwachung der Prozesse der Webserveranwendung wichtig, um den Gesamtzustand des Services für den Zugriff auf Kundenkonten korrekt ermitteln zu können.

Es scheint zunächst verhältnismäßig einfach, entsprechend der Überwachung der Geräteverfügbarkeit eine weitere Ressourcenüberwachung hinzuzufügen, um die Bedingung des Prozessmodells für den Webserver zu kontrollieren und die Verfügbarkeit der einzelnen Prozesse separat zu behandeln. In der folgenden Tabelle sind die potenziellen Fehlerszenarien sowie die Auswirkungen jeder Kombination auf die Verfügbarkeit der Webserver im Hinblick auf die Verarbeitung eines Prozesses aufgeführt. Diese Tabelle veranschaulicht eine Richtlinie, die auch als „Anfälligkeitsrichtlinie“ bezeichnet wird.

Matrix für den Servicezustand – Server und Prozesse

Webserver 1	Webserver 2	Prozess 1	Prozess 2	Web-Servicezustand
VERBUNDEN	VERBUNDEN	NORMAL	NORMAL	AKTIV
VERBUNDEN	VERBUNDEN	KRITISCH	NORMAL	VERSCHLECHTERT
VERBUNDEN	VERBUNDEN	NORMAL	KRITISCH	VERSCHLECHTERT
VERBUNDEN	VERBUNDEN	KRITISCH	KRITISCH	AUSGEFALLEN
UNTERBROCHEN	VERBUNDEN	KRITISCH	NORMAL	VERSCHLECHTERT
UNTERBROCHEN	VERBUNDEN	KRITISCH	KRITISCH	AUSGEFALLEN
UNTERBROCHEN	UNTERBROCHEN	KRITISCH	KRITISCH	AUSGEFALLEN

In der folgenden Tabelle sind die einzelnen Geräte und Prozesse durch die Ressourcenüberwachung ersetzt, mit der sie jeweils überwacht werden können.

Matrix für den Servicezustand – Geräte und Prozesse

SERVERGERÄTE	SERVERPROZESSE	WEBSERVICE
AKTIV	AKTIV	AKTIV
AKTIV	VERSCHLECHTERT	VERSCHLECHTERT
AKTIV	AUSGEFALLEN	AUSGEFALLEN
VERSCHLECHTERT	VERSCHLECHTERT	VERSCHLECHTERT
VERSCHLECHTERT	AUSGEFALLEN	AUSGEFALLEN
AUSGEFALLEN	AUSGEFALLEN	AUSGEFALLEN
VERSCHLECHTERT	AKTIV	VERSCHLECHTERT
AUSGEFALLEN	AKTIV	AUSGEFALLEN
AUSGEFALLEN	VERSCHLECHTERT	AUSGEFALLEN

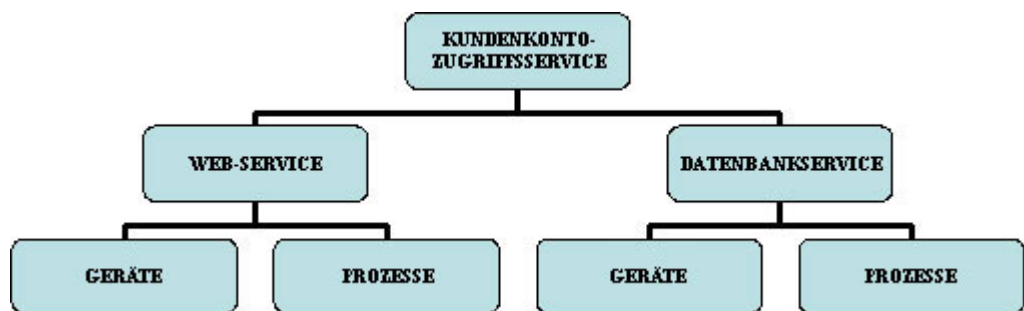
Hinweis: Die drei letzten Zeilen der Tabelle treffen in der Regel nicht zu, da in einem System, das als ausgefallen verzeichnet wird, keine Prozesse gemeldet werden sollten, die ausgeführt werden. Diese Fälle sollten jedoch auch mit den Regeln abgedeckt werden, um unbekannte Statuswerte zu vermeiden.

Im Hinblick auf die Geräte und Prozesse wird anhand der Tabelle deutlich, dass es sich hier um keinen Fall für eine Redundanzrichtlinie handelt, die bei der Auswertung der Ressourcen die erste Wahl zu sein schien. Wie im Fall des gesamten Services festgestellt wurde, umfasst die Beziehung zwischen Web-Servicehosts und Webserverprozessen einen Anfälligkeitsregelsatz, der dem folgenden ähnelt.

- Wenn eine Ressource ausfällt, fällt der Service aus.
- Wenn sich die Leistung einer Ressource verschlechtert, verschlechtert sich die Leistung des Services.

Nach der Auswertung dieser Beziehung zwischen den Servergeräten und -prozessen scheint die Erweiterung des Entwurfs von Beispiel 1 um zusätzliche Überwachungen, z. B. der neuen Prozessressourcenmodelle, nicht ohne weiteres möglich. Da im anfänglichen Entwurf versucht wurde, einen Service auf oberer Ebene mit mehreren Komponenten zu umfassen, wurden Subservices innerhalb des Services für den Zugriff auf Kundenkonten nicht erkannt. Nach der Erweiterung der Überwachung auf die Prozessebene wurde deutlich, dass ein Websubservice und ein Datenbankservice vorhanden sind. Sie können die Hostanwendung für Datenbankserver in ähnlicher Weise wie Webserver überwachen. Wenn die Ressourcenüberwachung auf die Prozessebene erweitert wird, bildet sich eine Hierarchie heraus.

Servicehierarchie



In der Regel werden Services auf unterer Ebene erkannt, die zunächst nicht bedeutsam genug für ein Servicemodell erschienen. Im Allgemeinen ist der Vorgang der Servicemodellierung ein schrittweiser Prozess. Mit jeder Berichtigung wird die Genauigkeit erhöht und die Gesamtanzahl der Fehlerszenarien erweitert, die korrekt verzeichnet werden können.

Dieser schrittweise Ansatz kann auf verschiedene Weise zusammengefasst werden. Eine Möglichkeit besteht darin, die Zielsetzung jeder Berichtigung so festzulegen, dass die Ursacheninformationen erweitert werden, die im Falle eines Servicefehlers verfügbar sind. Wenn in Beispiel 1 beide Webservergeräte verfügbar sind, ein Webserverprozess jedoch ausfällt, meldet der Service keinen Fehler, obwohl die Benutzer des Services wahrscheinlich einen gewissen Leistungsabfall feststellen. Durch die Erweiterung der Überwachung auf die Prozessebene meldet der Service nun die Verschlechterung und gibt den Prozessfehler als Ursache an. Im nächsten Abschnitt ist dargestellt, wie Beispiel 2 in SPECTRUM implementiert werden kann.

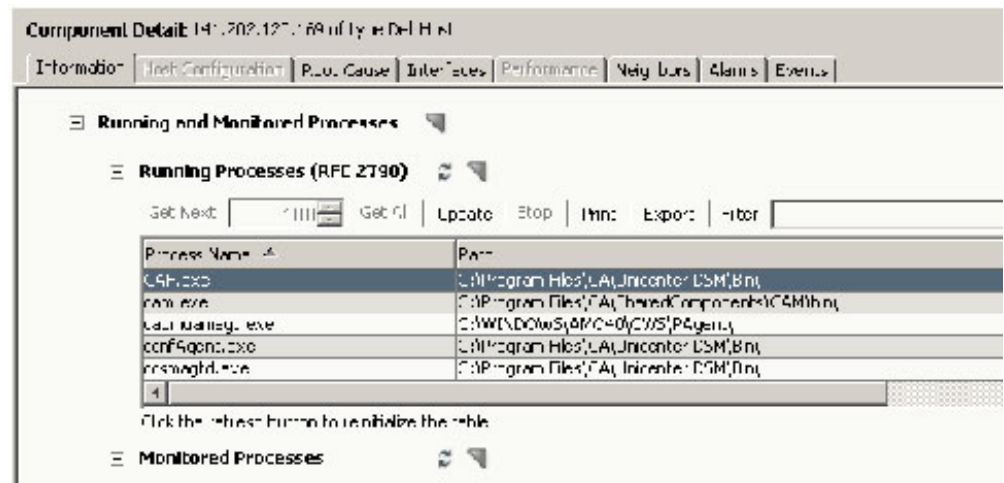
Implementierung von Beispiel 2 in SPECTRUM

Der Entwurf für Beispiel 2 beinhaltet die Erstellung von vier Prozessmodellen. Mit zwei Prozessmodellen wird die Webserveranwendung überwacht, mit den anderen beiden Modellen die Datenbankserveranwendung. Wahrscheinlich identifiziert ein Benutzer weitere Prozesse, die sich auf die Verfügbarkeit einer bestimmten Servicekomponente auswirken. Dieser Ansatz kann erweitert werden, so dass auch weitere Prozesse eingebunden werden.

Wenn Sie Prozessmodelle erstellen möchten, suchen Sie das Hostmodell, das den Server darstellt, auf dem der entsprechende Prozess ausgeführt wird. Im Beispiel handelt es sich dabei um ein Modell für Webserver- oder Datenbankservergeräte. Wenn der Agent auf dem Gerät RFC 2790 unterstützt, können Sie Prozessmodelle für jeden gewünschten zu überwachenden Prozess erstellen.

So erstellen Sie ein Prozessmodell für jeden Prozess:

1. Zeigen Sie in der SPECTRUM OneClick-Konsole den Host oder die Hosts im OneClick-Fenster „Contents“ an.
2. Wählen Sie den Host aus, für den Sie eine Überwachungsregel erstellen möchten.
3. Erweitern Sie den Bereich „System Resources“ in der OneClick-Ansicht „Component Detail“. Der untergeordnete Bereich „Running and Monitored Processes“ wird angezeigt.
4. Erweitern Sie die Ansicht „Running and Monitored Processes“, so dass der Bereich „Running Processes“ angezeigt wird, in dem wiederum eine Tabelle mit Prozessen eingeblendet wird.



Hinweis: Wenn bei den Bezeichnungen der Bereiche der Text „(RFC 2790)“ nicht angezeigt wird, unterstützt der Agent die RFC 2790-Erweiterung für MIB-II nicht. Sie können dann auf dem entsprechenden Host keine Prozesse überwachen und keine Alarme auslösen, wenn Prozesse gestartet oder beendet werden.

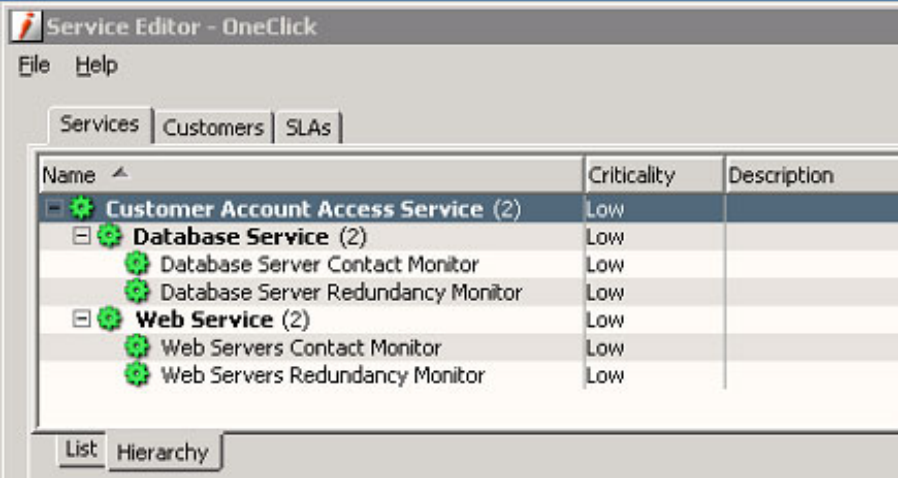
- a. Klicken Sie in der Tabelle mit der rechten Maustaste auf einen Prozess, und wählen Sie „Monitor this process“ aus. Das Dialogfeld „Add Monitored Process“ wird angezeigt.
- b. Wählen Sie „Alarm on Stop“ aus, und klicken Sie auf „OK“. Mit dieser Einstellung wird ein kritischer Alarm im Prozessmodell ausgelöst, wenn der entsprechende Prozess beendet wird. Der Prozess wird in der Ansicht „Monitored Processes“ angezeigt.

5. Starten Sie nach dem Erstellen des entsprechenden Prozessmodells den Service Editor, indem Sie „Tools“, „Utilities“ und dann „Service Editor“ auswählen oder indem Sie mit der rechten Maustaste auf einen Prozess klicken und dann „Utilities“ und „Service Editor“ auswählen. Der in Beispiel 1 erstellte Service soll so geändert werden, dass dieser komplexere Fall verarbeitet werden kann. Es sollen ähnliche Schritte wie in Beispiel 1 ausgeführt werden, jedoch mit einer erweiterten Hierarchie, bei der eine neue mittlere Schicht sowie Logik für die Prozesse hinzugefügt werden.
 - > Erstellen Sie mit Hilfe der Condition Value Map und der Redundanzrichtlinie den Service zur Überwachung der Webserverredundanz, mit dem die Prozessmodelle für Webserver überwacht werden.
 - > Erstellen Sie mit Hilfe der Anfälligkeitsrichtlinie für den Servicezustand den Web-Service, mit dem die Verbindungsüberwachung für Webserver und die Überwachung der Webserverredundanz überwacht werden. Dazu muss die Unterordnung der Verbindungsüberwachung für Webserver vom Service für den Zugriff auf Kundenkonten wieder auf diesen Service verlagert werden.
 - > Kopieren Sie diese Aufgaben für die Überwachung der Datenbankserverredundanz und für den Datenbankservice.

Mit dem Service für den Zugriff auf Kundenkonten werden nun der Web-Service und der Datenbankservice mit der in der Implementierung von Beispiel 1 beschriebenen Standardrichtlinie für den Kontenzugriff überwacht.

ÜBERBLICK BEISPIEL 2

In Beispiel 2 wurde die Überwachung des Service für den Zugriff auf Kundenkonten um die Überwachung des eigentlichen Webserverprozesses erweitert. In diesem Beispiel werden zudem zwei verschiedene Subservices innerhalb des Service für den Zugriff auf Kundenkonten aufgezeigt. Jeder dieser Subservices umfasst mehrere Ressourcen, die unterschiedlich überwacht werden, wie in der folgenden hierarchischen Ansicht von Service Editor dargestellt ist.



Name	Criticality	Description
Customer Account Access Service (2)	Low	
Database Service (2)	Low	
Database Server Contact Monitor	Low	
Database Server Redundancy Monitor	Low	
Web Service (2)	Low	
Web Servers Contact Monitor	Low	
Web Servers Redundancy Monitor	Low	

In der folgenden Tabelle ist die ständig steigende Zahl der Fehlerszenarien aufgeführt, die mit der vorhandenen Servicemodellierung unterstützt werden können.

Matrix für den Servicezustand – Fehlerszenarien

Legende:

- **WSG** Webservergerät
- **WSP** Webserverprozess
- **DBG** Datenbankgerät
- **DBP** Datenbankprozess
- **ZSK** Service für den Zugriff auf Kundenkonten
- **VS** Verschlechterter Servicezustand
- **GV** Geringfügig verschlechterter Servicezustand
- **AF** Ausgefallener Service

WSG1	WSG2	WSP1	WSP2	DBG1	DBG2	DBP1	DBP2	ZSK
AKTIV	AKTIV	AKTIV	AKTIV	AKTIV	AKTIV	AKTIV	AKTIV	AKTIV
AKTIV	AF	AKTIV	AF	AKTIV	AKTIV	AKTIV	AKTIV	GV
AF	AKTIV	AF	AKTIV	AKTIV	AKTIV	AKTIV	AKTIV	GV
AKTIV	AKTIV	AF	AKTIV	AKTIV	AKTIV	AKTIV	AKTIV	GV
AKTIV	AKTIV	AKTIV	AF	AKTIV	AKTIV	AKTIV	AKTIV	GV
AKTIV	AKTIV	AKTIV	AKTIV	AF	AKTIV	AF	AKTIV	GV
AKTIV	AKTIV	AKTIV	AKTIV	AKTIV	AF	AKTIV	AF	GV
AKTIV	AKTIV	AKTIV	AKTIV	AKTIV	AKTIV	AF	AKTIV	GV
AKTIV	AKTIV	AKTIV	AKTIV	AKTIV	AKTIV	AKTIV	AF	GV
AF	AKTIV	AF	AKTIV	AF	AKTIV	AF	AKTIV	VS
AF	AKTIV	AF	AKTIV	AKTIV	AF	AKTIV	AF	VS
AKTIV	AF	AKTIV	AF	AF	AKTIV	AF	AKTIV	VS
AKTIV	AF	AKTIV	AF	AKTIV	AF	AKTIV	AF	VS
AKTIV	AKTIV	AF	AKTIV	AKTIV	AKTIV	AF	AKTIV	VS
AKTIV	AKTIV	AF	AKTIV	AKTIV	AKTIV	AKTIV	AF	VS
AKTIV	AKTIV	AKTIV	AF	AKTIV	AKTIV	AF	AKTIV	VS
AKTIV	AKTIV	AKTIV	AF	AKTIV	AKTIV	AKTIV	AF	VS
AF	AF	AF	AF	AKTIV	AKTIV	AKTIV	AKTIV	AF

WSG1	WSG2	WSP1	WSP2	DBG1	DBG2	DBP1	DBP2	ZSK
AF	AF	AF	AF	AF	AKTIV	AF	AKTIV	AF
AF	AF	AF	AF	AKTIV	AF	AKTIV	AF	AF
AKTIV	AKTIV	AF	AF	AKTIV	AKTIV	AKTIV	AKTIV	AF
AKTIV	AKTIV	AF	AF	AF	AKTIV	AF	AKTIV	AF
AKTIV	AKTIV	AF	AF	AKTIV	AF	AKTIV	AF	AF
AKTIV	AKTIV	AF	AF	AKTIV	AKTIV	AF	AKTIV	AF
AKTIV	AKTIV	AF	AF	AKTIV	AKTIV	AF	AF	AF
AF	AF	AF	AF	AF	AF	AF	AF	AF

In der Tabelle sind 25 verschiedene Fehlerszenarien aufgeführt, die in der Implementierung von Beispiel 2 gemeldet werden können. Beachten Sie das Szenario oben in der fett formatierten Zeile. In diesem Szenario sind bei allen kritischen Prozessen Fehler aufgetreten. In diesem Fall fällt der Service aus, in der Implementierung von Beispiel 1 wird er jedoch nicht als ausgefallen gemeldet.

Beispiel 3: Erweiterung des Services zur Einbindung eines Antwortzeitelements

Mit Beispiel 2 wurde der Service für den Zugriff auf Kundenkonten um die Sichtbarkeit auf Prozessebene erweitert. In einigen Fällen wird der Service nicht optimal ausgeführt, obwohl die Geräte aktiv sind und die Prozesse ausgeführt werden. Es empfiehlt sich häufig, ein gewisses Maß an Leistungsüberwachung als Ressource der Servicekomponenten einzubinden. Dies ist insbesondere dann wichtig, wenn der Servicezustand die Wahrnehmung des Endbenutzers beim Verwenden des Services widerspiegeln soll.

In diesem Beispiel wird ein Antwortzeitelement zur Web-Servicekomponente des Services für den Zugriff auf Kundenkonten hinzugefügt. Durch Hinzufügen des Leistungselements wird nicht nur die Serviceüberwachung verbessert, sondern auch die Modularität des in Beispiel 2 erstellten Entwurfs getestet. Eine Zielsetzung des Serviceentwurfs sollte darin bestehen, Services zu erstellen, die bei zunehmenden Einblicken in die Aspekte der Überwachung der einzelnen Services auf einfache Weise erweitert werden können.

Das Hinzufügen der Antwortzeitkomponente beinhaltet das Erstellen von Antwortzeittestmodellen in SPECTRUM. Viele Geräte und Systemagenten unterstützen Antwortzeittests. Da mit diesem Beispiel die Überwachung der Web-Servicekomponente erweitert werden soll, erstellen Sie HTTP-Antwortzeittests.

Die Anzahl der Tests kann je nach Entwurf unterschiedlich ausfallen. Es empfiehlt sich in der Regel, für jeden Webserver mindestens eine HTTP-Anforderung zu erstellen. Sie können beispielsweise zwei SPM-Testhosts auswählen und zwei HTTP-Tests für jeden Testhost konfigurieren. Der Testhost sollte Anforderungen an jeden Webserver ausgeben. Dadurch werden mehrere Anforderungspunkte für jeden einzelnen Server bereitgestellt. Die vier neuen Antwortzeittests ergeben zusammen eine neue Ressourcengruppe innerhalb des Web-Services.

Es liegen zwei typische Ansätze zur Überwachung von Antwortzeittests vor:

- Überwachen des jeweils letzten Fehlerstatus der einzelnen Antwortzeittestmodelle
- Überwachen der kumulierten Ergebniswerte der einzelnen Testmodelle

Der zweite Ansatz wird später ausführlich erörtert. In diesem Beispiel werden die jeweils letzten Fehlerstatuswerte der einzelnen Testmodelle überwacht. In der folgenden Tabelle sind die letzten Fehlerstatuswerte (Antwortzeitwerte) dem entsprechenden Servicezustand zugeordnet. Dieser Prozess wird in SPECTRUM Service Manager weitgehend verwendet. Das Ziel besteht darin, reine Attributwerte mit vergleichbaren Servicezustandswerten zu vereinheitlichen, die dann einfach auf verschiedene Regelsätze angewendet werden können.

Matrix für den Servicezustand – Antworttests

Antwortzeitwert	Entsprechender Servicezustand
OK	AKTIV
TIMEOUT	KRITISCH
SCHWELLENWERT KRITISCH	KRITISCH
SCHWELLENWERT SCHWERWIEGEND	VERSCHLECHTERT
SCHWELLENWERT GERINGFÜGIG	GERINGFÜGIG VERSCHLECHTERT

In einigen Fällen werden in der Dokumentation möglicherweise zulässige Antwortzeitebenen angegeben. Wenn dies nicht der Fall ist, empfiehlt es sich, Antwortzeittests ohne Schwellenwerte zu erstellen und die Wartezeit in einem bestimmten Zeitraum zu überprüfen. Dadurch können Sie Grundswellenwerte erstellen und so sicherstellen, dass ein ungewöhnlicher Wartezeitwert eine Schwellenwertverletzung nach sich zieht.

In Beispiel 2 wurde der Web-Service entwickelt, um eine Ressourcenüberwachung für den Verbindungsstatus der Webservergeräte und eine Ressourcenüberwachung für die Bedingung der Webserverprozessmodelle einzubinden. Es ist unter Umständen möglich, die Überwachung des Web-Services so zu erweitern, dass die Antwortzeitkomponente eingebunden wird, indem lediglich eine dritte Ressourcenüberwachung hinzugefügt wird, mit der die Antwortzeittestmodelle kontrolliert werden.

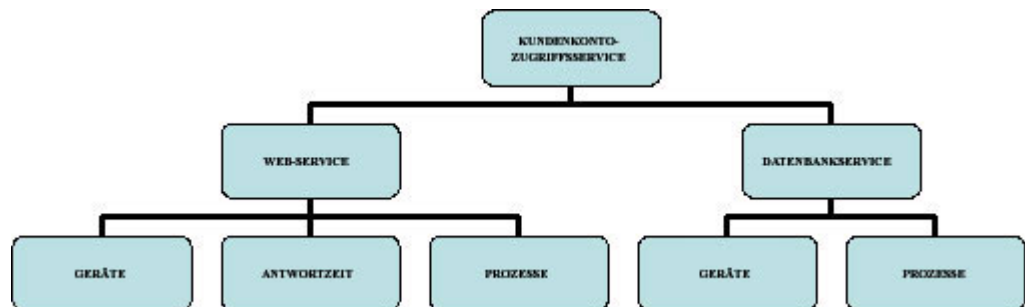
Bei der Überwachung dieser Antwortzeittestmodelle empfiehlt sich die Verwendung des folgenden Regelsatzes:

- Wenn alle Ressourcen ausfallen, fällt der Service aus.
- Wenn eine Ressource ausfällt, verschlechtert sich die Leistung des Services.
- Wenn sich die Leistung aller Ressourcen verschlechtert, verschlechtert sich die Leistung des Services.

Dieser Regelsatz wirkt sich folgendermaßen auf die weiter oben beschriebenen Antwortzeittests aus:

- Wenn sich bei allen Antwortzeittests eine Zeitlimit- oder kritische Schwellenwertverletzung ergibt, wird dadurch angegeben, dass über keinen der Webserver eine Antwort erfolgen konnte. Dabei handelt es sich eindeutig um ein kritisches Szenario, bei dem ein ausgefallener Service angegeben werden sollte.
- Wenn bei einem Antwortzeittest ein Zeitlimit oder ein kritischer Schwellenwert überschritten wird, wird dadurch angegeben, dass einer der Webserver so beeinträchtigt war, dass Anforderungen nicht angemessen verarbeitet werden konnten. In Anbetracht der Tatsache, dass einige andere Antwortzeittests erfolgreich durchgeführt werden, kann davon ausgegangen werden, dass der Service nicht vollständig ausfällt, sondern sich lediglich verschlechtert.
- Wenn bei keinem der Tests ein Zeitlimit oder ein kritischer Schwellenwert überschritten wird, jedoch bei allen ein schwerwiegender Schwellenwert überschritten wird, können Sie davon ausgehen, dass sich der Servicezustand verschlechtert.

Sie können den Web-Service auf der Grundlage der oben festgelegten Konfiguration erweitern, indem Sie eine neue Ressourcenüberwachung für die Antwortzeittests hinzufügen. Die Web-Servicekomponente wird dann in allen oben beschriebenen Fällen ordnungsgemäß ausgeführt. Beim Überwachen der zugehörigen Ressourcen mit der Anfälligkeitsrichtlinie für den Servicezustand verursacht jede ausgefallene Ressourcenüberwachung den Ausfall des Web-Services. Ebenso zieht die Verschlechterung einer jeden Ressource die Verschlechterung des Web-Services nach sich. Der in Beispiel 2 erstellte Entwurf kann also auf einfache Weise um das Antwortzeitelement erweitert werden. Im Folgenden ist beispielhaft die Servicehierarchie nach dem Hinzufügen der Antwortzeitkomponente zum Web-Service abgebildet.



IMPLEMENTIERUNG VON BEISPIEL 3 IN SPECTRUM

Bei diesem Beispiel erstellen Sie vier HTTP-Antwortzeittests. Auf der Registerkarte „Locator“ der OneClick-Konsole können Sie Hosts für Antwortzeittests suchen. Das Menü „Locator“ enthält eine Reihe vorkonfigurierter SPM-Suchvorgänge.

Hinweis: Wenn Sie einen HTTP-Test durchführen möchten, müssen Testquellen wie SystemEDGE-Agenten mit Service Availability, Cisco IP SLA-fähige Router oder Network Harmoni-Agenten mit Hilfe von Community-Zeichenfolgen mit Lese-Schreib-Zugriff erkannt werden. Ausführliche Informationen zu Antwortzeittests und zu unterstützten Agenten finden Sie im *Service Performance Manager User Guide*.

So erstellen Sie Antwortzeittests:

1. Suchen Sie über „All Test Hosts“ Testhostmodelle, mit denen HTTP-Antwortzeiten für die Webserver gemessen werden können. (Erweitern Sie im Fenster „Contents“ die Optionen „SPM Searches“ und „Test Hosts By“, klicken Sie mit der rechten Maustaste auf „All Test Hosts“, und wählen Sie dann „Launch the selected search“ aus.)
2. Erstellen Sie für jeden vorgesehenen Testhost neue HTTP-Tests, indem Sie in der Tabelle mit der rechten Maustaste auf den entsprechenden Host klicken, „New Test“ und dann „HTTP“ auswählen.
3. Geben Sie die Daten für die Schwellenwerte an. Konfigurieren Sie die Schwellenwerte so, dass sichergestellt wird, dass ein kritischer Schwellenwert generiert wird, wenn die Antwortzeit nicht mehr zulässig ist, und dass ein schwerwiegender Schwellenwert generiert wird, wenn die Antwortzeit zwar noch zulässig, jedoch sehr langsam ist. Fügen Sie als Ziel für den Test einen der Webserverhosts hinzu.
4. Die Antwortzeittests können Sie mit Hilfe von Service Editor hinzufügen, indem Sie eine neue Ressourcenüberwachung, die Antwortzeitüberwachung für Webserver, hinzufügen, bei der die Anfälligkeitsrichtlinie für Antwortzeiten verwendet wird. Die Ressourcen können durch Erweitern von „SPM Searches“ gesucht werden. Anschließend können Sie die vier Antwortzeittests zur neuen Ressourcenüberwachung hinzufügen. Ordnen Sie diese neue Ressource schließlich dem Web-Service zu.

ÜBERBLICK BEISPIEL 3

In Beispiel 3 wird beschrieben, wie Sie eine vorhandene Serviceimplementierung um eine komplexere Ressourcenüberwachung erweitern können, ohne die Servicehierarchie zu ändern. Dieser flexible Entwurf der Servicehierarchie ermöglicht Benutzern, ihre Servicemodelle auf sehr einfache Weise kontinuierlich zu verbessern. Darüber hinaus wird in Beispiel 3 umrissen, wie eine Antwortzeitkomponente in einen Service eingebunden wird, um die Genauigkeit der Berichterstellung hinsichtlich des Servicezustands erheblich zu verbessern. Erneut wurde die Unterstützung der möglichen Fehlerszenarien sowie die Anzahl potenzieller Ursachen für Serviceeinbußen erweitert.

Erstellung von SLAs

In diesem Abschnitt werden Konzepte und Verfahren der SLA-Modellierung eingeführt, mit denen Sie sich vor der Modellierung von SLAs vertraut machen sollten.

Hinweis: Die folgenden Abschnitte einschließlich Beispiel 4 enthalten Anweisungen zum Verfolgen von SLAs anhand von Geschäftszeiten. Dieser Funktionsumfang ist in SPECTRUM 8.1 enthalten. Eine vollständige Beschreibung der verfügbaren Funktionen finden Sie im *Service Performance Manager User Guide*.

Die wichtigsten Konzepte

- **SLA-Zeiträume** SLAs bestehen aus einer Reihe von Service-Level-Zielen oder Gewährleistungen, die in einem bestimmten Zeitraum erfasst werden. Üblicherweise entspricht dieser Zeitraum einem eindeutigen Abrechnungs- oder Berichterstellungszyklus. Häufig beläuft sich ein SLA-Zeitraum auf einen Monat (d. h., die Einhaltung eines SLA wird monatlich bewertet). In der Regel wird die Einhaltung oder Verletzung eines SLA im Hinblick auf einen bestimmten Zeitraum erfasst. Die Einhaltung eines SLA wird beispielsweise für den Monat Januar verzeichnet. Wenn ein wöchentlicher Zeitraum festgelegt ist, wurde das SLA beispielsweise in der Woche vom 5. bis 11. November verletzt.

■ **SLA-Gewährleistungen oder Service-Level-Ziele** Neben anderen Bestimmungen umfasst ein SLA mehrere Gewährleistungen oder Service-Level-Ziele. Viele dieser Gewährleistungen beziehen sich im Besonderen auf die Verfügbarkeit und Leistung eines bestimmten Services oder einer Gruppe von Services. In einer typischen Umgebung von Serviceanbietern werden mit SLAs häufig sehr spezifische Gewährleistungen festgesetzt. Benutzer lesen unter Umständen Bestimmungen wie etwa: „...bestätigt eine monatliche Betriebszeit von 99,9 %...“ oder „...erstattet dem Kunden 1/30 der monatlichen Servicegebühr für den Fall, dass der Kunde einen Ausfall des Services von mindestens 30 Minuten meldet...“. Dabei handelt es sich jeweils um Gewährleistungen von Anbietern eines spezifischen Services. SLAs sind auch in der Unternehmensumgebung festgelegt, diese Unternehmens-SLAs sind jedoch möglicherweise weniger formal. Sehr häufig liegen SLAs wie „...die IT-Abteilung garantiert eine maximale Ausfallzeit des Webzugriffs von 30 Minuten pro Woche...“ vor. In beiden Fällen bilden diese Gewährleistungen oder Service-Level-Ziele die Grundlage für die Festlegung der SLA-Einhaltung mit SPECTRUM.

■ **Aktive SLA-Überwachung** Im Gegensatz zu anderen SLA-Managementprodukten wird mit SPECTRUM Service Manager ein aktives SLA-Management bereitgestellt. Dies bedeutet, dass Sie in einem bestimmten Zeitraum den Status des SLA in diesem Zeitraum ermitteln können. Anhand von Ausfalltendenzen wird der voraussichtliche Status für den gesamten Zeitraum angezeigt. Zu Beginn jedes SLA-Zeitraums wird ein SLA als nicht betroffen eingestuft. Der nicht betroffene Status bleibt bestehen, bis für das SLA aufgrund eines Ausfalls eine Ausfallzeit im entsprechenden Zeitraum erfasst wird. Ein SLA, bei dem eine Ausfallzeit erfasst wurde, die jedoch kein wesentliches Risiko für eine Verletzung darstellt, wird als konform gekennzeichnet.

Wenn innerhalb des Zeitraums weitere Ausfallzeiten auftreten und sich so häufen, dass eine Verletzung des SLA möglich wird, erhält das SLA einen Warnstatus. Wenn im Zeitraum weiterhin Ausfallzeiten auftreten und bestimmte Gewährleistungsschwellenwerte erreicht werden, erhält das SLA einen Verletzungsstatus. Dieser Übergang von einem nicht betroffenen Status zu einem Verletzungsstatus erfolgt in Echtzeit. Wenn der SLA-Zeitraum für einen Monat festgelegt ist und das SLA am fünften Tag verletzt wird, erkennen Sie die Verletzung des SLA unmittelbar und müssen nicht auf den Bericht am Ende des Zeitraums warten, in dem die Verletzung angegeben ist. Aufgrund dieser aktiven SLA-Überwachung können Serviceanbieter Maßnahmen ergreifen, bevor SLAs verletzt werden.

■ **SLA-Geltungszeit oder Geschäftszeiten** Innerhalb des SLA-Zeitraums wird häufig eine bestimmte Gewährleistung geltend gemacht. Das SLA enthält möglicherweise Angaben wie „...gewährleistet, dass die Ausfallzeit zwischen 8:00 Uhr und 17:00 Uhr von Montag bis Freitag eine Dauer von 30 Minuten nicht überschreitet...“ Derartige Angaben werden im Allgemeinen als Gewährleistungen für Geschäftszeiten bezeichnet. Manchmal werden mehrere Gewährleistungen für bestimmte Zeitrahmen festgelegt. Zum Beispiel „...gewährleistet eine Verfügbarkeit von 97,5 % 7 Tage/24 Stunden mit einer Verfügbarkeit von 99,9 % zwischen 8:00 Uhr und 17:00 Uhr Montag bis Freitag und zwischen 8:00 Uhr und 12:00 Uhr am Samstag...“ Obwohl es sich um den gleichen Service handelt, beinhaltet diese Angabe zwei Gewährleistungen: eine Gewährleistung für den Zeitrahmen 7 Tage/24 Stunden und eine zweite Gewährleistung für spezifische Stunden in der Woche.

Erstellung von SLAs und Gewährleistungen

Der erste Schritt beim Erstellen eines SLA umfasst die Einordnung des spezifischen Services, dem das SLA zugeordnet ist, sowie des Zeitraums, in dem das SLA gilt. Die Hierarchie der Servicemodellierung beinhaltet häufig ein Servicemodell auf oberster Ebene, das logisch einem SLA zugeordnet ist. In der Umgebung von Serviceanbietern ist beispielsweise der Service auf oberer Ebene „Kunde A – Schnelle Datenübertragung“ festgelegt.

Das SLA ist daher die Verbindlichkeit des schnellen Datenübertragungsservices, der Kunde A zur Verfügung gestellt wird. Der spezifische Zeitraum kann in einem SLA-Dokument oder beliebig festgelegt werden, es muss sich jedoch um einen zeitlichen Rahmen handeln, den Serviceanbieter und Servicekunde gemeinsam vereinbart haben. Im Allgemeinen wird ein monatlicher SLA-Zeitraum festgelegt, da dieser häufig einem Abrechnungszyklus des Services entspricht. Ein SLA-Zeitraum kann beispielsweise ab dem Ersten eines Monats gelten, wobei sich die Gewährleistungen auf die Verfügbarkeit und Leistung in dem entsprechenden Monat beziehen. In der Regel sind in einem SLA Erstattungsgewährleistungen festgelegt, wenn sich Kunden in einem Streitfall innerhalb einer bestimmten Anzahl von Tagen ab dem Ende eines bestimmten Zeitraums an den Serviceanbieter wenden.

Nach der Festlegung des Services auf oberer Ebene sowie des SLA-Zeitraums sollten Sie die SLA-Gewährleistungen oder Service-Level-Ziele hinsichtlich der Verfügbarkeit und Leistung des erbrachten Services identifizieren. Häufig finden Sie diese Gewährleistungen im SLA-Dokument unter anderen Bestimmungen, die sich nicht auf die Verfügbarkeit oder Leistung eines Services beziehen. Suchen Sie die Bestimmungen, die Angaben zum Grad der Verfügbarkeit, zu einer garantierten Antwortzeit, einer zulässigen Wartezeit o. Ä. enthalten. Darüber hinaus sollten Sie prüfen, ob diese Bestimmungen andere Festlegungen enthalten, in denen bestimmte Zeiten innerhalb des SLA-Zeitraums angegeben werden, in denen die Bestimmungen gewährleistet sind.

Nach dem Herausarbeiten der Gewährleistungen in einem SLA können Sie sie nach Verfügbarkeit und Antwortzeit untergliedern. Verfügbarkeitsgewährleistungen in einem SLA werden häufig prozentual angegeben. Sie können jedoch auch im Hinblick auf Ausfallzeiten beschrieben werden. Zum Beispiel „...Ausfallzeit von maximal 1 Stunde...“. Gewährleistungen für Antwortzeiten zeichnen sich beispielsweise durch Angaben wie „...Antwortzeit von maximal 2000 ms...“ oder „...in einem Zeitraum von 30 Minuten wird eine Wartezeit von 5000 ms nicht überschritten...“ aus.

Verfügbarkeit kann auf verschiedene Weise beschrieben werden. In einigen Abschnitten weiter oben in diesem Dokument wurde der Zustand von Services erörtert. Im Allgemeinen lässt sich Verfügbarkeit im Hinblick auf einen Service so beschreiben, dass der Service verfügbar ist, wenn kein Ausfall zu verzeichnen ist, oder dass der Service nicht verfügbar ist, wenn er ausfällt. Eine Verfügbarkeitsgewährleistung kann jedoch auch so festgelegt werden, dass ein Service nicht verfügbar ist, wenn er nicht reagiert. Diese zweite Beschreibung kann beim Erstellen von Gewährleistungsmodellen von sehr großer Bedeutung sein.

Gewährleistungen für Antwortzeiten umfassen Services, bei denen Antwortzeitkomponenten als zugehörige Ressourcen eingesetzt werden. Interessant an Gewährleistungen für Antwortzeiten ist, dass mit Komponenten innerhalb einer Servicehierarchie Antwortzeiten speziell dazu überwacht werden können, um eine Gewährleistung für Antwortzeiten in einem SLA zu unterstützen. Hierbei handelt es sich um ein sehr häufig vorkommendes Szenario.

Oft gründet eine Servicehierarchie auf den Ressourcen, die die physischen Geräte und Anwendungen umfassen, mit denen ein Service für Benutzer zur Verfügung gestellt wird. Antwortzeittests, mit denen der Servicezustand zwar optimal erfasst werden kann, werden häufig jedoch erst als Servicere Ressourcen identifiziert, wenn ein SLA zur Anwendung kommt, in dem Gewährleistungen für Antwortzeiten festgelegt sind. Wie bereits weiter oben erwähnt, können Sie mit Hilfe von Antwortzeitüberwachungen hohe Wartezeiten oder Serviceverschlechterungen ermitteln. Mit Antwortzeittests sollten schwerwiegende Schwellenwertverletzungen erfasst werden, wenn die zulässige Wartezeit überschritten wird. Zudem können Sie mit Hilfe von Antwortzeitüberwachungen kritische Bedingungen erfassen, wenn die Wartezeit eine nicht verwendungsfähige Ebene erreicht oder das Zeitlimit von Antwortzeitanforderungen überschritten wird. Wenn Sie dies beim Erstellen von Antwortzeitüberwachungen berücksichtigen, kann mit diesen sowohl die Wartezeit als auch die Verfügbarkeit überwacht werden.

Für den Fall, dass ein Service als nicht verfügbar gilt, wenn er nicht reagiert, kann mit einem zur Erfassung von Antwortzeiten erstellten Service auch die Verfügbarkeit ermittelt werden, obwohl die Gewährleistung eines zur Erfassung der Verfügbarkeit konzipierten Services nie für Antwortzeiten gilt.

Beispiel 4: Ein SLA für den 'Service für den Zugriff auf Kundenkonten'

In diesem Abschnitt wird ein Beispiel auf der Grundlage des Services für den Zugriff auf Kundenkonten erörtert, der weiter oben entworfen wurde. Es beinhaltet ein SLA und mehrere Gewährleistungen.

Im Abschnitt zur Erstellung von Servicemodellen in diesem Kapitel wurde der Service für den Zugriff auf Kundenkonten implementiert. Bei diesem Beispiel stellt der Service für den Zugriff auf Kundenkonten den Service eines fiktiven Unternehmens mit dem Namen „Northeast Data Solutions“ dar (im Folgenden als „Northeast“ bezeichnet).

Northeast verwaltet Kundendaten für zahlreiche Kleinunternehmen. Jedes Kleinunternehmen ist zuständig für die Erstellung und Pflege seiner Kundendaten. Northeast übernimmt die Verantwortung für den Support und die Sicherung der Kundendaten. Neben der Unterstützung der Datenbanken und des Webzugriffs führt Northeast zudem Verhandlungen mit verschiedenen Internet Service Anbietern (Internet Service Providers, ISPs) zur Bereitstellung eines lokalen Routers für den Remote-Kundenstandort, um sicherzustellen, dass den Kunden für den Zugriff auf ihre Kontodaten eine zuverlässige Internetverbindung zur Verfügung steht. Die Beziehung mit den ISPs ist für Kunden von Northeast transparent. Die Kunden bezahlen den Service direkt an Northeast.

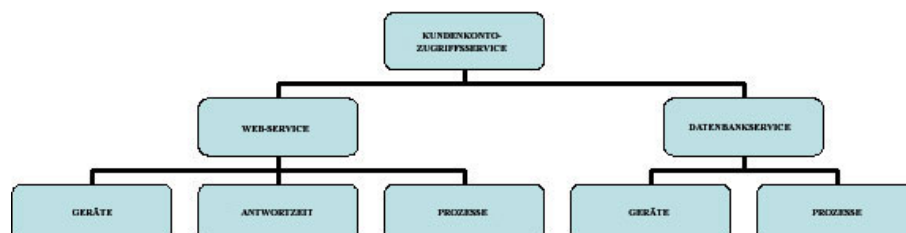
Im Folgenden sind Ausschnitte des SLA aufgeführt, das für alle Kunden von Northeast Datenlösungen gilt:

- Northeast Data Solutions stellt den Zugriff auf die Daten der Kundenkonten bereit und garantiert, dass der Kontenzugriff an allen Kundenstandorten 99 % der monatlichen Zeit verfügbar ist. Davon ausgenommen sind die für Systemwartungen eingeplanten Zeiträume jeden Sonntag zwischen 0:00 Uhr und 03:00 Uhr.
- Die Serviceverfügbarkeit muss umgehend wiederhergestellt werden. Die durchschnittliche Dauer bis zur Wiederinbetriebnahme nach einem Ausfall sollte maximal 30 Minuten betragen, wobei einzelne Ausfälle die Dauer einer Stunde nicht überschreiten sollten. Darüber hinaus wird garantiert, dass innerhalb von 24 Stunden nicht mehr als 2 Ausfälle auftreten.
- Die regulären Geschäftszeiten gelten für einen wöchentlichen Zeitrahmen von Montag bis Freitag, 7:00 Uhr bis 18:00 Uhr.
- Während der regulären Geschäftszeiten ist die Verfügbarkeit des Kontenzugriffs 99,5 % der Zeit garantiert. Einzelne Ausfälle dauern nicht länger als 20 Minuten.
- Die durchschnittliche Transaktionszeit für den initialen Kontenzugriff sollte die Dauer von 5 Sekunden für mehr als 5 % des Zeitrahmens der regulären Geschäftszeiten nicht überschreiten, wobei für 99 % der regulären Geschäftszeiten der erfolgreiche Abschluss der Transaktion garantiert wird. Eine Transaktion gilt als erfolgreich, wenn sie innerhalb von 15 Sekunden abgeschlossen wurde und während der Transaktion keine Ausfallzeiten von mehr als 20 Minuten auftreten.
- Die durchschnittliche Transaktionsüberwachung basiert auf einer Stichprobe von fünf Abfragen, die während der regulären Geschäftszeiten nach dem Zufallsprinzip in einem 5-Minuten-Intervall ausgewählt werden. Alle Abfragen stammen von der Zugriffseinheit des Kunden.
- Northeast übernimmt die Verantwortung für ein Zugriffsgerät. Die Betriebsfähigkeit des Geräts wird garantiert. Davon ausgenommen sind Stromausfälle oder Fälle höherer Gewalt, die außerhalb der Kontrolle von Northeast liegen.

In diesem Beispiel enthält der SLA-Text eine Reihe von Gewährleistungskriterien und -begriffen mit fiktiven charakteristischen Bestimmungen, die auch in tatsächlichen SLAs festgelegt sind. Trotz der verwirrenden Begrifflichkeit umfasst dieses SLA einige sehr präzise Gewährleistungsangaben, darunter die genaue Erfassung der Antwortzeiten.

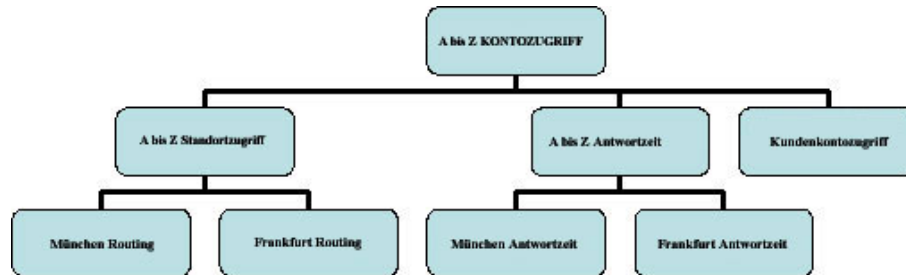
Dieses SLA gilt für alle Kunden von Northeast. Dieses Beispiel konzentriert sich jedoch auf das SLA zwischen Northeast und einem Kunden mit dem Namen „A to Z Performance Components“ mit Geschäftsstellen in Atlanta und Savannah, Georgia.

Wie bereits erwähnt, besteht der erste Schritt beim Entwerfen einer SLA-Implementierung in der Einordnung des Services und des Zeitraums für das SLA. In der folgenden Abbildung ist die Hierarchie des Services für den Zugriff auf Kundenkonten dargestellt.



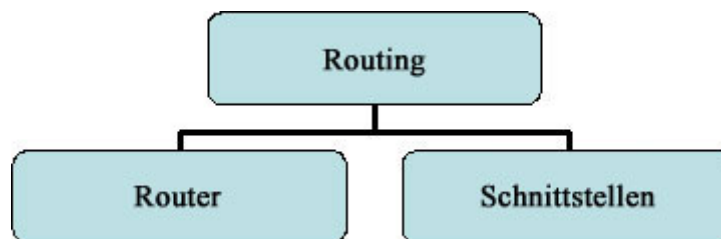
Zur Überwachung der Serviceverfügbarkeit von A to Z bedarf es vieler Komponenten. Neben der Bereitstellung des Web- und Datenbankzugriffs muss Northeast nun Servicekomponenten erstellen, mit denen die Verfügbarkeit und die Antwortzeiten überwacht werden, die jeweils für die Geschäftsstellen von A to Z in Atlanta und Savannah spezifisch sind.

Mit diesen neuen Servicekomponenten werden Zugriffsroutern an jedem Standort sowie die Antwortzeiten für neu erstellte Antwortzeittests überwacht, die auf den Zugriffsroutern an jedem Standort durchgeführt werden. In der folgenden Abbildung ist dargestellt, wie Sie die Hierarchie zur Unterstützung von A to Z erweitern können.



Die Bewertung des SLA impliziert, dass eine Reihe von Gewährleistungen festgelegt wurden und dass einige neue Servicemodelle erforderlich werden. Diese Abbildung stellt nur eine mögliche zu verwendende Konfiguration dar. Überprüfen Sie jede SLA-Implementierung sorgfältig, um die beste Möglichkeit zum Strukturieren der Services herauszuarbeiten.

Zu den neuen Services zählt eine Hierarchie mit dem Namen „A to Z Site Access“. A to Z Site Access umfasst zwei Subservices mit den Namen „Atlanta Routing“ und „Savannah Routing“. Mit diesen Services soll jeweils der Router vor Ort überwacht werden, über den auf den Service für den Zugriff auf Kundenkonten zugegriffen werden kann. Sie können jeden dieser Subservices in mehrere Ressourcenüberwachungen unterteilen, so dass eine Hierarchie ähnlich der in der folgenden Abbildung entsteht.



Mit einer Ressourcenüberwachung wird der Verbindungsstatus des Routers kontrolliert, während mit der anderen Ressourcenüberwachung der Port Status der Interfaces des Routers kontrolliert wird, die entscheidend für den Zugriff am Standort sind. Der Routingsservice wird als ausgefallen gekennzeichnet, wenn der Router ausfällt oder wenn alle erforderlichen Interfaces deaktiviert sind. Ein ähnlicher Service soll auch für Atlanta und Savannah implementiert werden. Gemäß SLA gelten folgende Festlegungen für die Routing-Komponenten beider Standorte:

- Northeast stellt den Zugriff auf die Daten der Kundenkonten bereit und gewährleistet, dass der Kontenzugriff an allen Kundenstandorten zu 99 % der monatlichen Zeit verfügbar ist. Davon ausgenommen sind die Zeiträume, die für Systemwartungen eingeplant sind, sonntags zwischen 0:00 Uhr und 3:00 Uhr.

- Die Serviceverfügbarkeit muss umgehend wiederhergestellt werden, so dass die durchschnittliche Ausfallzeit bis zur Wiederinbetriebnahme maximal 30 Minuten (oder weniger) beträgt, wobei einzelne Ausfälle nicht länger als eine Stunde andauern sollten. Weiterhin wird gewährleistet, dass innerhalb von 24 Stunden nicht mehr als 2 Ausfälle auftreten.

Die Gewährleistungen werden jeweils pro Standort gegeben. Den Benutzern des Service Managers soll beispielsweise im Monat November eine Verfügbarkeit von 99 % gewährleistet werden. Damit ist insgesamt eine Ausfallzeit von 432 Minuten zulässig. Wenn Sie das SLA erstellen, sollten Sie sich genau überlegen, für welche(n) Service(s) das SLA gelten soll. Angenommen, die Gewährleistung soll für den Service „A to Z Site Access“ gelten, und in Atlanta treten Ausfallzeiten von 300 Minuten und in Savannah treten Ausfallzeiten von 200 Minuten (was einer Gesamtausfallzeit von 500 Minuten entspricht) auf. In diesem Fall liegt eindeutig eine Verletzung des SLA vor. Da das SLA jedoch die Formulierung „...jeder Kundenstandort..“, enthält, bezieht sich die Gewährleistung jeweils auf die einzelnen Standorte. Wenn die Gültigkeit der Gewährleistung in dieser Weise definiert wird, liegt in dem obigen Fall keine SLA-Verletzung vor, weil die zulässige Ausfallzeit von 432 Minuten an keinem der Standorte überschritten wird. Für den Routing-Service werden zwei verschiedene Gewährleistungen mit jeweils 99 %iger Verfügbarkeit definiert:

- Atlanta: 99 % Verfügbarkeit
- Savannah: 99 % Verfügbarkeit

Das SLA besagt weiter, dass „...die durchschnittliche Ausfallzeit bis zur Wiederinbetriebnahme nicht mehr als 30 Minuten betragen darf...“. Mit der Gewährleistung der 99 %igen Verfügbarkeit ist jedwede zusätzliche Gewährleistung, die eine durchschnittliche Ausfallzeit von 30 Minuten oder weniger vorsieht, hinfällig. Die entsprechende Komponente kann als MTTR-Zusatz (durchschnittliche Reparaturzeit) in die Verfügbarkeitsgewährleistungen aufgenommen werden. Die Verfügbarkeitsgewährleistungen enthalten nun die folgende MTTR-Klausel:

- Atlanta: 99 % Verfügbarkeit, MTTR 30 Minuten
- Savannah: 99 % Verfügbarkeit, MTTR 30 Minuten

In Ergänzung zur MTTR-Komponente wird in dem SLA weiter gewährleistet, „... dass innerhalb von 24 Stunden nicht mehr als 2 Ausfälle auftreten...“. Diese Festlegung wird als MTBF-Klausel (Mean Time Between Failures) bezeichnet. Die MTBF-Klausel gibt an, dass pro Tag maximal ein Ausfall auftreten darf. Die Verfügbarkeitsgewährleistungen enthalten nun auch folgende MTBF-Klausel:

- Atlanta: Verfügbarkeit 99 %, MTTR 30 Minuten, MTBF 24 Stunden
- Savannah: Verfügbarkeit 99 %, MTTR 30 Minuten, MTBF 24 Stunden

Eine ähnliche Gewährleistung sollte auch für den Service für den Zugriff auf Kundenkonten definiert werden, wobei diese jedoch unabhängig vom Kundenstandort formuliert werden sollte:

- Atlanta: Verfügbarkeit 99 %, MTTR 30 Minuten, MTBF 24 Stunden
- Savannah: Verfügbarkeit 99 %, MTTR 30 Minuten, MTBF 24 Stunden
- Zugriff auf Kundenkonten: Verfügbarkeit 99 %, MTTR 30 Minuten, MTBF 24 Stunden

Zusätzlich zu der Gewährleistung einer Gesamtverfügbarkeit von 99 % sollten weitere Festlegungen zur Verfügbarkeit definiert werden, z. B.:

- Die regulären Geschäftszeiten umfassen einen wöchentlichen Zeitraum von Montag bis Freitag, von 7:00 Uhr bis 18:00 Uhr.
- Während der regulären Geschäftszeiten sollte der Kontenzugriff zu 99,5 % der Zeit verfügbar sein, wobei einzelne Ausfälle nicht länger als 20 Minuten dauern sollten.

Die Gewährleistungen zu den Geschäftszeiten können mit Hilfe eines Zeitplans erstellt werden. Für neue Gewährleistungen gilt ein wöchentlicher Zeitplan von Montag bis Freitag, 7:00 Uhr bis 18:00 Uhr, wobei für den gesamten Planungszeitraum eine Verfügbarkeit von 99,5 % garantiert wird.

Die neuen Gewährleistungen sollten sowohl für die Routingservices der Kunden als auch für den Service für den Zugriff auf Kundenkonten definiert werden:

- Atlanta: Verfügbarkeit 99 %, MTTR 30 Minuten, MTBF 24 Stunden
- Savannah: Verfügbarkeit 99 %, MTTR 30 Minuten, MTBF 24 Stunden
- Zugriff auf Kundenkonten: Verfügbarkeit 99 %, MTTR 30 Minuten, MTBF 24 Stunden
- Atlanta: Verfügbarkeit 99,5 %, M-F 7:00-18:00 Uhr
- Savannah: Verfügbarkeit 99,5 %, M-F 7:00-18:00 Uhr
- Zugriff auf Kundenkonten: Verfügbarkeit 99,5 %, M-F 7:00-18:00 Uhr

Die Gewährleistung für die Geschäftszeiten sollte eine zusätzliche Festlegung enthalten, dass „einzelne Ausfälle die Dauer von 20 Minuten nicht überschreiten dürfen...“. Diese Festlegung wird auch als MOT-Klausel (Maximum Outage Time) bezeichnet. Die Gewährleistungen für die Geschäftszeiten enthalten nun auch folgende MOT-Klausel:

- Atlanta: Verfügbarkeit 99 %, MTTR 30 Minuten, MTBF 24 Stunden
- Savannah: Verfügbarkeit 99 %, MTTR 30 Minuten, MTBF 24 Stunden
- Zugriff auf Kundenkonten: Verfügbarkeit 99 %, MTTR 30 Minuten, MTBF 24 Stunden
- Atlanta: Verfügbarkeit 99,5 %, M-F 7:00-18:00 Uhr, MOT 20 Minuten
- Savannah: Verfügbarkeit 99,5 %, M-F 7:00-18:00 Uhr, MOT 20 Minuten
- Zugriff auf Kundenkonten: Verfügbarkeit 99,5 %, M-F 7:00-18:00 Uhr, MOT 20 Minuten

Bis zu diesem Punkt wurden sechs verschiedene Verfügbarkeitsgewährleistungen identifiziert, wobei jedoch in keiner dieser Gewährleistungen das Antwortzeitelement innerhalb des SLA berücksichtigt wurde:

- Die durchschnittliche Transaktionszeit für den initialen Kontenzugriff sollte die Dauer von 5 Sekunden für mehr als 5 % des Zeitrahmens der regulären Geschäftszeiten nicht überschreiten, wobei für 99 % der regulären Geschäftszeiten der erfolgreiche Abschluss der Transaktionen garantiert wird. Eine Transaktion gilt als erfolgreich, wenn sie innerhalb von 15 Sekunden abgeschlossen wurde und während der Ausführung keine Ausfallzeiten von mehr als 20 Minuten auftreten.
- Die durchschnittliche Transaktionsüberwachung basiert auf einer Stichprobe von fünf Abfragen, die während der regulären Geschäftszeiten nach dem Zufallsprinzip in einem 5-Minuten-Intervall ausgewählt werden. Alle Abfragen stammen von der Zugriffseinheit des Kunden.

Die Festlegungen zur Antwortzeit sind sehr umfangreich und geben an, wie die Antwortzeit gemessen wird. Zur Unterstützung dieser SLA-Komponente müssen Sie zwei weitere Services erstellen, die die Antwortzeittests als überwachte Ressourcen verwenden.

Erstellen Sie für Atlanta einen Antwortzeitservice, um fünf neue Antwortzeittestmodelle zu überwachen, die auf dem Zugangsrouter von Atlanta verwaltet und in 5-Minuten-Intervallen ausgeführt werden. Das SLA legt fest, dass die 5-Sekunden-Marke und die 15-Sekunden-Marke jeweils schwerwiegende bzw. kritische Schwellenwerte darstellen. Möglicherweise gehen Sie daher davon aus, dass die einzelnen Antwortzeittests (SPM-Tests) jeweils mit der 5-Sekunden-Marke als schwerwiegendem und der 15-Sekunden-Marke als kritischem Schwellenwert konfiguriert werden sollten. Die Formulierung des SLA legt jedoch nahe, dass dies nicht zweckmäßig wäre. Beachten Sie folgende Formulierung: „...Die durchschnittliche Transaktionszeit für den initialen Kontozugriff sollte die Dauer von 5 Sekunden nicht überschreiten...“. Statt der jeweiligen Antwortzeiten der einzelnen Tests sollte die durchschnittliche Antwortzeit überwacht werden.

Angenommen, für die Antwortzeiten wird folgende Ergebnismenge ermittelt: 4 Sekunden, 3 Sekunden, 3 Sekunden, 3 Sekunden und 6 Sekunden. Durch das 6-Sekunden-Ergebnis wird der 5-Sekunden-Schwellenwert verletzt. Da die durchschnittliche Antwortzeit jedoch weniger als 4 Sekunden beträgt, wird die Vorgabe insgesamt nicht verletzt. Wenn Sie diese Funktionsweise bevorzugen, sollten Sie keine Schwellenwerte für die einzelnen Antwortzeittests vorgeben. Erstellen Sie stattdessen einen neuen Antwortzeitservice, der eine Richtlinie enthält, mit der die Wartezeiten der einzelnen Antwortzeittests überwacht werden können. Die neue Servicerichtlinie sollte so definiert werden, dass bei allen Antwortzeittestmodellen das aktuelle Ergebnis überwacht wird. Zur Auswertung der Antwortzeiten sollte folgender aggregierter Regelsatz in der Richtlinie verwendet werden:

- Wenn der Durchschnittswert aller Ressourcen größer als 15000 ist, liegt ein Serviceausfall vor.
- Wenn der Durchschnittswert aller Ressourcen größer als 5000 ist, liegt ein Leistungsabfall des Services vor.

Der Wert des aktuellen Ergebnisses („Latest Result“) eines Antwortzeittestmodells ergibt sich aus der Anzahl der Millisekunden, die benötigt wurden, um den letzten Test abzuschließen. Daher werden die Werte in der oben beschriebenen Servicerichtlinie in Millisekunden angegeben. Diese Richtlinie sollte für den Antwortzeitservice von Atlanta und den Antwortzeitservice von Savannah eingesetzt werden, um die fünf Antwortzeittests, die jeweils auf den Routern für den Sitezugriff verwaltet werden, zu überwachen.

Gemäß den Antwortzeitspezifikationen des SLA müssen zwei Antwortzeitgewährleistungen für die Geschäftszeiten definiert werden, mit denen die Antwortzeiten der oben erstellen Services nachverfolgt werden:

- Atlanta: Antwortzeit 95 %, M-F 7:00-18:00 Uhr
- Savannah: Antwortzeit 95 %, M-F 7:00-18:00 Uhr

Die Antwortzeitklausel wird durch folgende zusätzliche Verfügbarkeitskomponente ergänzt:

- ...der erfolgreiche Abschluss von Transaktionen ist während der regulären Geschäftszeiten zu 99 % zu gewährleisten. Eine Transaktion gilt als erfolgreich, wenn sie innerhalb von 15 Sekunden abgeschlossen wurde und während der Transaktion keine Ausfallzeiten von mehr als 20 Minuten auftreten.

Wenn man die zweite Festlegung der Verfügbarkeitsgewährleistung berücksichtigt, die besagt, „dass ein Service als nicht verfügbar gilt, wenn er nicht reagiert“, muss die obige SLA-Spezifikation durch zwei weitere Gewährleistungen der 99 % igen Verfügbarkeit, inklusive MOT-Klausel, erweitert werden:

- Atlanta: Antwortzeit 95 %, M-F 7:00-18:00 Uhr
- Savannah: Antwortzeit 95 %, M-F 7:00-18:00 Uhr
- Atlanta: Verfügbarkeit 99 %, M-F 7:00-18:00 Uhr, MOT 20 Minuten
- Savannah: Verfügbarkeit 99 % M-F 7:00-18:00 Uhr, MOT 20 Minuten

Darüber hinaus sollte eine Klausel zu Wartungszeitfenstern in das SLA aufgenommen werden:

- Davon ausgenommen sind die Zeiträume, die für Systemwartungen eingeplant sind, sonntags zwischen 0:00 Uhr und 3:00 Uhr.

Zur Berücksichtigung der Wartungszeitfenster müssen Sie die einzelnen Services so modifizieren, dass der Zeitplan für Wartungen in diesen Zeitraum einbezogen wird.

In der folgenden Tabelle werden alle SLA-Komponenten aufgeführt, die in diesem Entwurf berücksichtigt wurden:

Entwurf der SLA-Komponenten

SERVICE:	SLA-KOMPONENTE:
A to Z Account Access	Monatliches SLA
Customer Account Access	Verfügbarkeit 99 %, MTTR 30 Minuten, MTBF 24 Stunden Verfügbarkeit 99,5 %, M-F 7:00-18.00 Uhr, MOT 20 Minuten
Atlanta Routing	Verfügbarkeit 99 %, MTTR 30 Minuten, MTBF 24 Stunden Verfügbarkeit 99,5 %, M-F 7:00-18:00 Uhr, MOT 20 Minuten
Savannah Routing	Verfügbarkeit 99 %, MTTR 30 Minuten, MTBF 24 Stunden Verfügbarkeit 99,5 %, M-F 7:00-18:00 Uhr, MOT 20 Minuten
Atlanta Response Time	Antwortzeit 95 %, M-F 7:00-18:00 Uhr Verfügbarkeit 99 %, M-F 7:00-18:00 Uhr, MOT 20 Minuten
Savannah Response Time	Antwortzeit 95 %, M-F 7:00-18:00 Uhr Verfügbarkeit 99 %, M-F 7:00-18:00 Uhr, MOT 20 Minuten

Implementierung des SLA für A to Z Account Access in SPECTRUM

Zur Implementierung des im letzten Abschnitt beschriebenen SLA-Entwurfs müssen Sie folgende grundlegenden Schritte ausführen:

1. Erstellen Sie die beiden Routingservices und die dazugehörigen Ressourcenüberwachungen für Router und Interfaces. Es werden 6 Services erzeugt, die in zwei Hierarchien unterteilt werden.
 - › Verwenden Sie den Service Editor, um für jeden Standort die erste Ressourcenüberwachung (Router von Atlanta und Router von Savannah) zu konfigurieren und den Kontaktstatus des Routergerätemodells mit Hilfe der Anfälligkeitsrichtlinie für den Kontaktstatus zu überwachen.
 - › Konfigurieren Sie für jeden Standort die zweite Ressourcenüberwachung (Interfaces von Atlanta und Interfaces von Savannah), um mit Hilfe der Richtlinie für den Portstatus der kritischen Router-Interfaces zu überwachen. Verwenden Sie entweder den Regelsatz „Low Sensitivity“ oder den Regelsatz „Percentage“ für die Servicerichtlinie, je nachdem, wie viele Interfacemodelle für die Bereitstellung des Zugriffs erforderlich sind.
 - › Erstellen Sie mit Hilfe des Service Editors die Routingservices für Atlanta und Savannah, um den Servicezustand der beiden (oben definierten) Ressourcenüberwachungen mit Hilfe der Anfälligkeitsrichtlinie für Servicezustände zu überwachen.
2. Erstellen Sie die Antwortzeitservices für Atlanta und Savannah sowie die dazugehörigen Antwortzeittest-/SPM-Modelle.
 - › Verwenden Sie die Registerkarte „Locator“ der OneClick-Konsole, um für jeden Standort 5 SPM-Testmodelle mit folgenden Einstellungen zu konfigurieren:
 - Ein Planungsintervall von 5 Minuten (300 Sekunden), mit deaktivierten Schwellenwerten
 - Ein Zeitlimit von 25-30 Sekunden
 - Setzen Sie „Filter Timeout Data“ auf „FALSE“, um die Testmodelle so zu konfigurieren, dass der Wert für das Zeitlimit in das aktuelle Ergebnis („Latest Result“) geschrieben wird.
 - › Erstellen Sie mit Hilfe des Service Editors die Antwortzeitservices für Atlanta und Savannah, und stellen Sie sicher, dass diese die neu erstellten Antwortzeittest-/SPM-Modelle überwachen.
 - › Konfigurieren Sie die beiden Antwortzeitservices mit Hilfe des Servicerichtlinien-Editors. Definieren Sie dazu eine neue Richtlinie, die das aktuelle Ergebnis des Antwortzeittests überwacht, sowie den folgenden aggregierten Regelsatz:
 - Wenn der Durchschnittswert aller Ressourcen größer als 15000 ist, liegt ein Serviceausfall vor.
 - Wenn der Durchschnittswert aller Ressourcen größer als 5000 ist, liegt ein Leistungsabfall des Services vor.

3. Fassen Sie Routing- und Antwortzeitservices sowie den kürzlich erstellten Service für den Kundenzugriff (aus Beispiel 2) zu Services auf höherer Ebene zusammen.
 - > Fassen Sie die Routing- und Antwortzeitservices beider Kundenstandorte zu den beiden neuen Services „A to Z Site Access“ und „A to Z Response Time“ zusammen. Die beiden neuen Services sollten ihre jeweiligen Komponenten mit Hilfe einer Anfälligkeitsrichtlinie für Servicezustände überwachen.
 - > Erstellen Sie den Service „A to Z Account Access“, um die Services „A to Z Site Access“, „A to Z Response Time“ und den „Customer Account Access“ zu überwachen. Die neuen Services sollten ihre jeweiligen Komponenten mit Hilfe einer Anfälligkeitsrichtlinie für Servicezustände überwachen.
4. Legen Sie die Regeln für das SLA fest.
 - > Nachdem Sie alle erforderlichen Änderungen an der Servicehierarchie vorgenommen haben, wechseln Sie zur Registerkarte „SLA“ des Service Editors. Erstellen Sie ein SLA für den Service „A to Z Account Access“, das für einen monatlichen SLA-Zeitraum gilt. Zu diesem Zeitpunkt sollten noch keine Gewährleistungen für den Service „A to Z Account Access“ definiert werden.
 - > Markieren Sie das neue SLA, und starten Sie den „Guarantee Editor“.
 - > Erstellen Sie mit Hilfe des „Guarantee Editor“ die zehn Gewährleistungen (8 Verfügbarkeitsgewährleistungen und 2 Antwortzeitgewährleistungen), die im letzten Abschnitt als relevant identifiziert wurden.
 - > Nehmen Sie die MTTR-, MTBF- und MOT-Spezifikationen in die entsprechenden Gewährleistungen auf.

Hinweis: Eine Funktion zur Verknüpfung der Gewährleistungen mit bestimmten Geschäftszeiten ist für SPECTRUM 8.1 vorgesehen. In älteren Versionen (vor 8.1) können Sie die Einschränkung für die Geschäftszeiten außer Acht lassen.

Verletzung der SLA-Gewährleistungen liegt in folgenden Fällen vor:

- Wenn der Schwellenwert einer Gewährleistung überschritten wird.
- Wenn der Schwellenwert einer zusätzlichen Gewährleistung (also MOT, MTTR, MTBF) überschritten wird.

Bei Überschreitung des MOT-Schwellenwerts wird das SLA automatisch infolge der zusätzlichen Gewährleistung verletzt. Wenn die Schwellenwerte für MTTR oder MTBF überschritten werden, wird das SLA infolge der Gewährleistung automatisch in den Status „gefährdet“ überführt, weil erst am Ende des SLA-Zeitraums endgültig feststeht, welcher der beiden Schwellenwerte, MTTR oder MTBF, verletzt wurde.

Der SLA-Status entspricht dem Status der Gewährleistung mit der geringsten Erfüllungsquote. Wenn eine Gewährleistung verletzt wird, wird gleichzeitig auch das SLA für den betreffenden SLA-Zeitraum verletzt. Bei Verlängerung des SLA-Zeitraums geht das SLA wieder in den Status „nicht betroffen“ über.

Eine Verletzung der SLA-Gewährleistungen liegt in folgenden Fällen vor:

- Wenn der Schwellenwert einer Gewährleistung überschritten wird.
- Wenn der Schwellenwert einer zusätzlichen Gewährleistung (also MOT, MTTR, MTBF) überschritten wird.

Bei Überschreitung des MOT-Schwellenwerts wird das SLA automatisch infolge der zusätzlichen Gewährleistung verletzt. Wenn die Schwellenwerte für MTTR oder MTBF überschritten werden, wird das SLA infolge der Gewährleistung automatisch in den Status „gefährdet“ überführt, weil erst am Ende des SLA-Zeitraums endgültig feststeht, welcher der beiden Schwellenwerte, MTTR oder MTBF, verletzt wurde.

Der SLA-Status entspricht dem Status der Gewährleistung mit der geringsten Erfüllungsquote. Wenn eine Gewährleistung verletzt wird, wird gleichzeitig auch das SLA für den betreffenden SLA-Zeitraum verletzt. Bei Verlängerung des SLA-Zeitraums geht das SLA wieder in den Status „nicht betroffen“ über.

Erstellung von Service- und SLA-Berichten

Serviceverfügbarkeits- und SLA-Berichte bilden einen zentralen Bestandteil der Servicemanagement-Lösung. Diese Berichte ergänzen den Modellierungsprozess für Services und SLAs und bieten einen Einblick in die Leistungsdaten der einzelnen Servicekomponenten, die über verschiedene Zeiträume erhoben werden. Service- und SLA-Berichte können in zwei Kategorien eingeteilt werden: kundennahe und interne Berichte.

Kundennahe Berichte stellen Informationen zur Serviceverfügbarkeit und zum SLA-Status zur Verfügung. Diese Berichte können an die Kunden des Services weitergegeben werden. SLAs enthalten häufig eine Festlegung, dass für alle SLA-Zeiträume separate Service- und SLA-Berichte an die Kunden übermittelt werden. Kundennahe Berichte bieten einen zusammenfassenden Überblick über den Status. In kundennahen Verfügbarkeitsberichten werden z. B. nur die beiden Kriterien Verfügbarkeitszeit und Ausfallzeit berücksichtigt. In gleicher Weise werden in kundennahen SLA-Berichten nur die Kriterien Erfüllung und Verletzung berücksichtigt.

Interne Berichte enthalten dagegen eine Fülle von Detaildaten, die Serviceanbietern oder Unternehmenskunden zur Verfügung gestellt werden. Im Gegensatz zu kundennahen Serviceverfügbarkeitsberichten werden in internen Serviceverfügbarkeitsberichten auch Wartungszeiten, Ausfallzeiten bei der Verwaltung usw. angezeigt. Darüber hinaus werden in den internen SLA-Berichten alle möglichen SLA-Status, z. B. „nicht betroffen“, „Konformitätswarnung“ und „verletzt“, berücksichtigt.

Andere interne Berichte bieten eine Zusammenfassung von Services mit den höchsten Ausfallzeiten bzw. von Servicere Ressourcen, die die höchsten Ausfallzeiten verursachen. Diese Berichte sollen einen Einblick in den Zustand und die Performance der betreffenden Services und SLAs innerhalb eines bestimmten Zeitraums gewähren.

Ausführung von kundennahen Berichten in SPECTRUM Service Manager

Für die Benutzer des Servicemanagements werden innerhalb der Kategorie Serviceverfügbarkeit und SLA verschiedene kundennahe Berichte bereitgestellt. Mit Hilfe des SPECTRUM Report Managers können Sie Ihre eigenen Berichte erstellen und verwalten. Der Zugriff auf diese Anwendung ist von allen Computern möglich, die über das Internet eine Verbindung mit dem OneClick-Server herstellen können, auf dem der Report Manager installiert ist.

So greifen Sie auf den Report Manager zu und führen Berichte aus:

1. Stellen Sie in einem Webbrowser eine Verknüpfung zum Report Manager her, indem Sie die URL `http://hostname/SPECTRUM/repmgr` eingeben (*hostname* entspricht dem Namen des OneClick- und Report Manager-Systems).
2. Melden Sie sich bei der Anwendung an, indem Sie im Anmeldefenster von OneClick Ihren Benutzernamen und Ihr Kennwort eingeben.
2. Klicken Sie im Begrüßungsbildschirm des Report Managers auf die Verknüpfung „Begin Session“.

Das Hauptfenster des Report Managers wird angezeigt. Das Hauptfenster bietet Zugriff auf alle Berichts- und Berichtsmanagementoptionen, die für Ihr Konto verfügbar sind. Dort werden alle geplanten Berichte aufgeführt, die bereits für Ihr Konto generiert wurden bzw. in nächster Zeit für das Konto generiert werden sollen. In den Textfeldern „Message of the Day“ und „What's New“ werden alle Meldungen angezeigt, die von den Report Manager-Administratoren veröffentlicht werden. Eine vollständige Beschreibung des Report Managers und seiner Verwendung finden Sie im Handbuch *Report Manager User Guide*.

In den folgenden Abschnitten werden die kundennahen Berichte vorgestellt.

Serviceverfügbarkeit nach: Name, Kunde, Eigentümer

Dieser Bericht zeigt ein 3D-Kreisdiagramm, das die prozentualen Anteile von Betriebszeit/Ausfallzeit und Verfügbarkeit während des Zeitraums angibt, für den der Bericht ausgeführt wurde. In einer Tabelle werden für alle Ausfälle Start- und Endzeit, Dauer sowie weitere Merkmale angegeben. Darüber hinaus wird für alle Ausfälle in der Tabelle ein Unterbericht mit detaillierten Informationen zu dem jeweiligen Ausfall bereitgestellt. Sie können verschiedene Serviceverfügbarkeitsberichte erstellen, die entweder nach Servicenamen, Servicekunden oder Serviceeigentümer angeordnet werden.

Date Range: 11/10/2006 12:00:00AM to 11/10/2006 10:18:27AM

[Customer Information For A to Z Performance Components](#)

Service Created: 11/10/2006 9:06:27AM
Service is Active:

Description: Monitors Atlanta site router and interfaces provided by North East Data Solutions.

Service Availability Summary



	TOTAL TIME	PERCENTAGE
AVAILABLE	0 Days + 01:08:24	96.26%
DOWN	0 Days + 00:02:36	3.61%
	0 Days + 01:12:00	

Start Time	End Time	Status	Duration	Details
Fri 11/10/06 10:07:29	Fri 11/10/06 10:07:30	Unplanned	0 Days + 00:01:31	▶
Fri 11/10/06 10:10:07	Fri 11/10/06 10:11:12	Unplanned	0 Days + 00:01:05	▶
Mean Time To Repair (MTTR): 0 Days + 00:01:01		Total Down Time: 0 Days + 00:02:36		
		Unplanned Down Time: 0 Days + 00:02:36		

Variable Health-Ebene für Serviceverfügbarkeit

Dieser Bericht weist zwar eine gewisse Ähnlichkeit zum Serviceverfügbarkeitsbericht auf, bietet jedoch die Möglichkeit, bei Bedarf auch verschlechterte bzw. geringfügig verschlechterte Antwortzeiten zu berücksichtigen. Ein 3D-Kreisdiagramm gibt die prozentualen Anteile der einzelnen Servicezustände während des Zeitraums an, für den der Bericht ausgeführt wurde. Die einzelnen Ausfälle werden in einem Unterbericht aufgeführt, der detaillierte Informationen zu dem jeweiligen Ausfall enthält.

SPECTRUM

Service Availability Report for SAVANNAH ROUTING

Date Range: 11/10/2006 12:00:00AM to 11/10/2006 10:22:18AM

[Customer Information For A to Z Performance Components](#)

Created: 11/10/2006 9:38:26AM

[Owner Information For serviceAdmin1](#)

Service is Active

Description: Monitors Savannah site router and interfaces. Provided by North East Data Solutions.

Service Health Summary



■ NORMAL
■ DOWN
■ DEGRADED
■ SLIGHTLY DEGRADED

TOTAL TIME PERCENTAGE

0 Days + 01:12:10 98.51%

0 Days + 00:01:06 1.08%

0 Days + 00:00:00 0.00%

0 Days + 00:00:00 0.00%

0 Days + 01:13:16

Outage	Start Time	End Time	Status	Duration	Details
Down	Fri 11/10/06 10:12:14	Fri 11/10/06 10:13:20	Unplanned	0 Days + 00:01:06	⏪
Down	Fri 11/10/06 10:20:10	Fri 11/10/06 10:21:30	Planned	0 Days + 00:01:20	⏪
Notes: Power failure at Savannah location. (root)					
Mean Time To Repair (MTTR): 0 Days + 00:01:18			Total Degrade Time: 0 Days + 00:02:28		
			Unplanned Down Time: 0 Days + 00:01:06		

Zusammenfassung der Services nach: Name, Kunde, Eigentümer

Dieser Bericht zeigt je nach Servicennamen, -kunden oder -eigentümer verschiedene Services einschließlich der dazugehörigen Ausfallzeiten und prozentualen Verfügbarkeit an.

SPECTRUM

Summary of Service Availability

Date Range: 17/10/2006 12:00:00 AM to 17/10/2006 10:36:03 AM

Service Name	Up	Down	Degraded	Slightly Degraded
At a/c Account Access				
Percentage	70.70%	13.52%	0.00%	7.28%
Total Time	0 Dy + 00:42:12	0 Dy + 00:07:10	0 Dy + 00:00:00	0 Dy + 00:03:53
Outage Count/ MTTR		0 / 0 Dy + 00:01:27	0 / 0 Dy + 00:00:00	2 / 0 Dy + 00:03:53
At a/c Site Access				
Percentage	100.00%	0.00%	0.00%	0.00%
Total Time	0 Dy + 01:03:17	0 Dy + 00:00:00	0 Dy + 00:00:00	0 Dy + 00:00:00
Outage Count/ MTTR		1 / 0 Dy + 00:01:15	0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00
At a/c Monitoring				
Percentage	100.00%	0.00%	0.00%	0.00%
Total Time	0 Dy + 01:17:50	0 Dy + 00:00:00	0 Dy + 00:00:00	0 Dy + 00:00:00
Outage Count/ MTTR		2 / 0 Dy + 00:01:15	0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00
Customer Account Access Service				
Percentage	100.00%	0.00%	0.00%	0.00%
Total Time	0 Dy + 00:39:34	0 Dy + 00:00:00	0 Dy + 00:00:00	0 Dy + 00:00:00
Outage Count/ MTTR		2 / 0 Dy + 00:01:12	0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00
Web Service				
Percentage	100.00%	0.00%	0.00%	0.00%
Total Time	0 Dy + 00:43:35	0 Dy + 00:00:00	0 Dy + 00:00:00	0 Dy + 00:00:00
Outage Count/ MTTR		1 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00	2 / 0 Dy + 00:01:11
Server at Reading				
Percentage	100.00%	0.00%	0.00%	0.00%
Total Time	0 Dy + 01:17:21	0 Dy + 00:00:00	0 Dy + 00:00:00	0 Dy + 00:00:00
Outage Count/ MTTR		1 / 0 Dy + 00:01:00	0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00
Database Service				
Percentage	100.00%	0.00%	0.00%	0.00%
Total Time	0 Dy + 00:47:18	0 Dy + 00:00:00	0 Dy + 00:00:00	0 Dy + 00:00:00
Outage Count/ MTTR		1 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00	1 / 0 Dy + 00:01:10
At a/c Backup Time				
Percentage	100.00%	0.00%	0.00%	0.00%
Total Time	0 Dy + 00:00:00	0 Dy + 00:00:00	0 Dy + 00:00:00	0 Dy + 00:00:00
Outage Count/ MTTR		0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00
Server at Reading Time				
Percentage	100.00%	0.00%	0.00%	0.00%
Total Time	0 Dy + 00:00:00	0 Dy + 00:00:00	0 Dy + 00:00:00	0 Dy + 00:00:00
Outage Count/ MTTR		0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00

Variable Health-Ebene für Zusammenfassung der Services

Dieser Bericht stellt eine Tabelle mit Services bereit, wobei in den Spalten der Tabelle, ähnlich wie im letzten Bericht, eine Zusammenfassung der Servicezustände angezeigt wird, die in dem Bericht berücksichtigt wurden. Sie können festlegen, ob nur die Daten zu den Ausfallzeiten angezeigt werden sollen, oder ob neben diesen Daten auch die verschlechterte oder geringfügig verschlechterte Performance in den Bericht aufgenommen werden soll. Für jeden in der Tabelle aufgeführten Service steht ein Unterbericht mit ausführlichen Informationen zu den Ausfällen zur Verfügung.

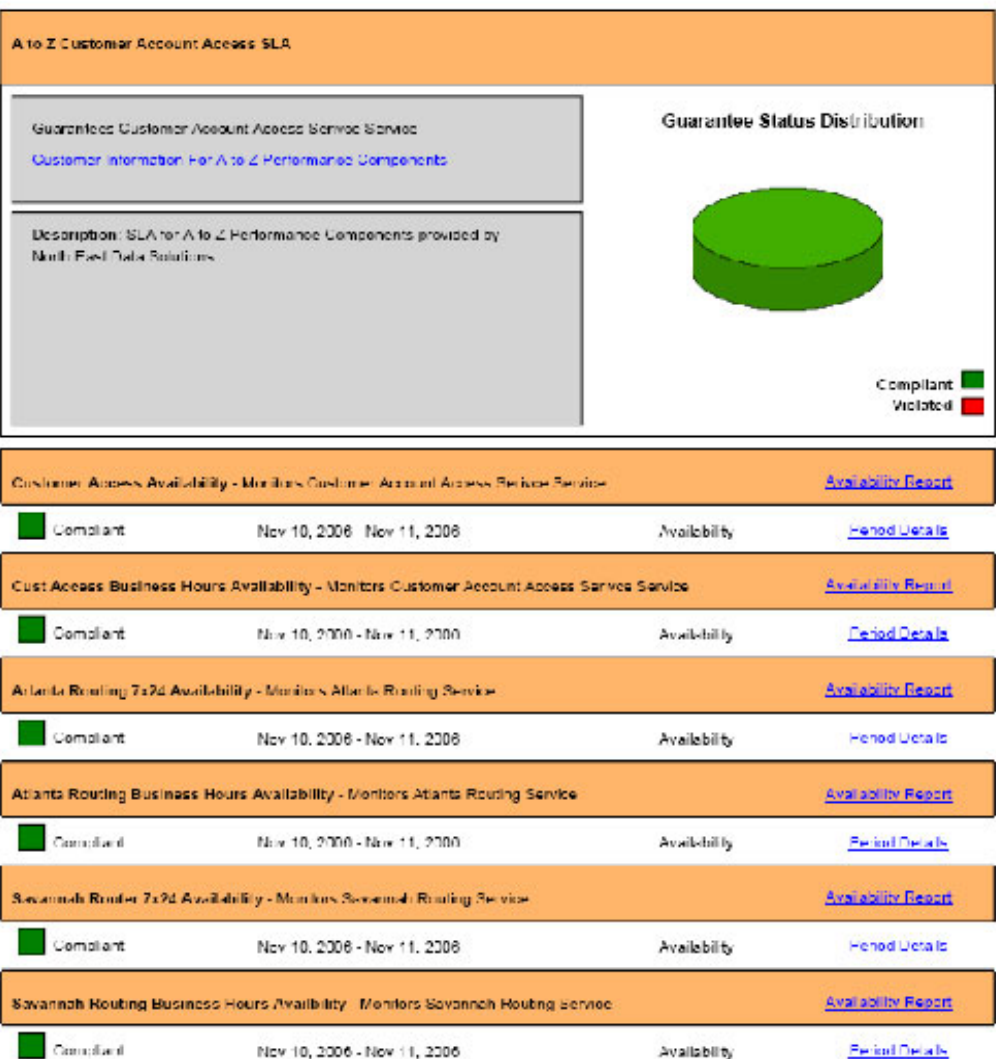
SLA-Details nach Kunden

Sie können diesen Bericht für einen oder mehrere SLA-Zeiträume erstellen. Der Bericht enthält ein Kreisdiagramm, in dem die prozentualen Gewährleistungen für alle erfassten Zeiträume angezeigt werden, die konform sind oder bei denen Verletzungen aufgetreten sind. Unterhalb des Diagramms sind alle Gewährleistungen mit dem jeweiligen Status der einzelnen Zeiträume aufgeführt. Für jeden Zeitraum können Sie einen Unterbericht öffnen, in dem detaillierte Informationen zu den Ausfällen einer bestimmten Gewährleistung aufgeführt sind, darunter auch Ausfallausnahmen. Wenn Sie den Bericht für einen Kunden ausführen, wird für die einzelnen SLAs des Kunden jeweils ein gesonderter Bericht erstellt. Sie können den Bericht dem Kunden am Ende jedes Zeitraums zur Verfügung stellen.

SPECTRUM

Service Level Agreement Detail Report

Date Range: 11/10/2006 12:00:00AM to 11/10/2006 3:00:12PM



SLA-Bestand nach Kunden

In diesem Bericht ist die Konfiguration der einzelnen SLAs und Gewährleistungen für einen bestimmten Kunden aufgeführt. Die Erstellung dieses Berichts für einen Kunden empfiehlt sich, wenn die SLA-Modelle und Gewährleistungsmodelle zum ersten Mal erstellt werden. Der Benutzer sollte die Konfiguration mit dem SLA-Dokument vergleichen können, um zu überprüfen, ob alle Gewährleistungen oder Service-Level-Ziele abgedeckt sind.

SPECTRUM

SLA Inventory Report for A to Z Performance Components

Report Generated: 11/10/2006 10:00:45AM

A to Z Customer Account Access SLA	Availability Threshold	Response Time Threshold	MAX Outage Time	Mean Time To Repair	Mean Time Between Faults
Customer Access Availability	0 Days + 00:14:34		0 Days + 00:00:00	0 Days + 00:00:00	1 Day + 00:00:00
Card Access Business Hours Availability	0 Days + 00:07:12		0 Days + 00:20:00	0 Days + 00:00:00	0 Days + 00:00:00
Atlanta Routing 7x24 Availability	0 Days + 00:14:34		0 Days + 00:00:00	0 Days + 00:00:00	1 Day + 00:00:00
Atlanta Routing Business Hours Availability	0 Days + 00:07:12		0 Days + 00:20:00	0 Days + 00:00:00	0 Days + 00:00:00
Savannah Router 7x24 Availability	0 Days + 00:14:34		0 Days + 00:00:00	0 Days + 00:00:00	1 Day + 00:00:00
Savannah Routing Business Hours Availability	0 Days + 00:07:12		0 Days + 00:20:00	0 Days + 00:00:00	0 Days + 00:00:00
Atlanta Response Time Business Hours Availability	0 Days + 00:14:34		0 Days + 00:20:00	0 Days + 00:00:00	0 Days + 00:00:00
Savannah Response Time Business Hours Availability	0 Days + 00:14:34		0 Days + 00:20:00	0 Days + 00:00:00	0 Days + 00:00:00
Atlanta Business Hours Response Time		0 Days + 00:10:00			
Savannah Business Hours Response Time		0 Days + 00:10:00			

SPECTRUM Service Manager: Interne Berichte

Für die Benutzer des Servicemanagements werden innerhalb der Kategorie Serviceverfügbarkeit und SLA verschiedene interne Berichte bereitgestellt. Die internen Berichte werden in den folgenden Abschnitten beschrieben.

Zustand von Services nach Servicename

Dieser Bericht weist eine große Ähnlichkeit mit einem Serviceverfügbarkeitsbericht auf, enthält jedoch Angaben zu allen Servicezuständen, einschließlich Wartung und Ausfall bei der Verwaltung. Der Bericht kann für Service- und Ressourcenüberwachungen gleichermaßen ausgeführt werden. In einem Kreisdiagramm sind die einzelnen Servicezustandswerte prozentual dargestellt. Dieser Bericht enthält auch eine Tabelle, in der die Ausfälle aller Servicezustandstypen aufgeführt sind, darunter Hinweise und Links für detaillierte Informationen zu den Ausfällen. Über den Servicezustandsbericht erhalten Benutzer von Service Manager sehr ausführliche Informationen zur Performance eines Services in einem bestimmten Zeitraum.

Date Range: 11/10/2006 12:00:00AM to 11/10/2006 10:23:18AM

Created: 11/10/2006 9:39:13AM

Service Is Active

Description: Monitors the overall availability of the Customer Account Access Service provided by North East Data Solutions.

Service Health Summary



	TOTAL TIME	PERCENTAGE
NORMAL	0 Days + 00:39:49	81.26%
DOWN	0 Days + 00:02:25	5.40%
DEGRADED	0 Days + 00:00:00	0.00%
SLIGHTLY DEGRADED	0 Days + 00:05:51	13.27%
MAINTENANCE	0 Days + 00:00:00	0.00%
LOSS OF MANAGEMENT	0 Days + 00:00:00	0.00%
	0 Days + 00:44:05	

Outage	Start Time	End Time	Status	Duration	Details
Down	Fri 11/10/06 10:07:30	Fri 11/10/06 10:07:40	Unplanned	0 Days + 00:00:10	⬅
Down	Fri 11/10/06 10:13:28	Fri 11/10/06 10:13:45	Unplanned	0 Days + 00:00:17	⬅
Mean Time To Repair (MTTR): 0 Days + 00:01:12			Total Down Time: 0 Days + 00:02:25 Unplanned Down Time: 0 Days + 00:02:25		
Outage	Start Time	End Time	Status	Duration	Details
Slightly Degraded	Fri 11/10/06 10:02:52	Fri 11/10/06 10:05:35	Unplanned	0 Days + 00:02:43	⬅
Slightly Degraded	Fri 11/10/06 10:07:40	Fri 11/10/06 10:09:38	Unplanned	0 Days + 00:01:58	⬅
Slightly Degraded	Fri 11/10/06 10:13:19	Fri 11/10/06 10:14:08	Unplanned	0 Days + 00:00:49	⬅
Mean Time To Repair (MTTR): 0 Days + 00:01:57			Total Slightly Degraded Time: 0 Days + 00:05:51 Unplanned Slightly Degraded Time: 0 Days + 00:05:51		

Inventar von Services

In diesem Bericht sind alle Services, Ressourcenüberwachungen und im System modellierten Ressourcen aufgegliedert. Er kann verwendet werden, um eine „Momentaufnahme“ der Serviceinventarkonfiguration des jeweils aktuellen Zeitpunkts zu speichern.

SPECTRUM

Service and Resource Monitor Inventory

Report Generated: 11/10/2006 10:58:05AM

Service Or Resource Monitor	Resources	Resource Class
(S) A to Z Account Access	(R) A to Z Site Access	Service Mgt Component
	(S) A to Z Site Resp Time	Service Mgt Component
	(S) Customer Account Access Service	Service Mgt Component
(S) A to Z Site Access	(S) Atlanta Routing	Service Mgt Component
	(R) Savannah Routing	Service Mgt Component
(S) A to Z Site Resp Time	(S) Atlanta Resp Time	Service Mgt Component
	(S) Savannah Response Time	Service Mgt Component
(S) Atlanta Resp Time	Atlanta Resp 1	Response Time Test
	Atlanta Resp 2	Response Time Test
	Atlanta Resp 3	Response Time Test
	Atlanta Resp 4	Response Time Test
	Atlanta Resp 5	Response Time Test
(S) Atlanta Routing	(RM) Router Contact	Service Mgt Component
	(RM) Port Status	Service Mgt Component
(S) Customer Account Access Service	(S) Web Service	Service Mgt Component
	(R) Database Service	Service Mgt Component
(S) Database Service	(RM) Devices	Service Mgt Component
	(RM) Processes	Service Mgt Component
(RM) Device	wlj018-scl	Workstation-Server
	HDMDYRKAPP02	Workstation-Server
(RM) Processes	RK4N7A01	Workstation-Server
	N13 HANSU HYNY	Workstation-Server
(RM) Port Status	G413PRR000_1TP_FID1	Port
	G016H8600_1/0_8600	Port

S - Indicates Service

RM - Indicates Resource Monitor

Report Generated: 11/10/2006 10:58:05AM

SPECTRUM SERVICE MANAGER

Page 1 of 2

Die Top-N-Services mit der schlechtesten Performance

Mit diesem Bericht können Sie die Top-N-Services mit der schlechtesten Performance für einen bestimmten Zeitraum anzeigen. In einem Balkendiagramm sind die Ausfallzeiten für die einzelnen Services zusammengefasst. Zudem enthält der Bericht eine Tabelle mit zusammengefassten Verfügbarkeitsinformationen für jeden Service. Diese Tabelle enthält auch Links zu einem detaillierteren Serviceverfügbarkeitsbericht. Dieser Bericht ist nützlich für Benutzer von Service Management, die Informationen zu den Services mit der schlechtesten Performance für bestimmte Zeiträume anzeigen möchten.

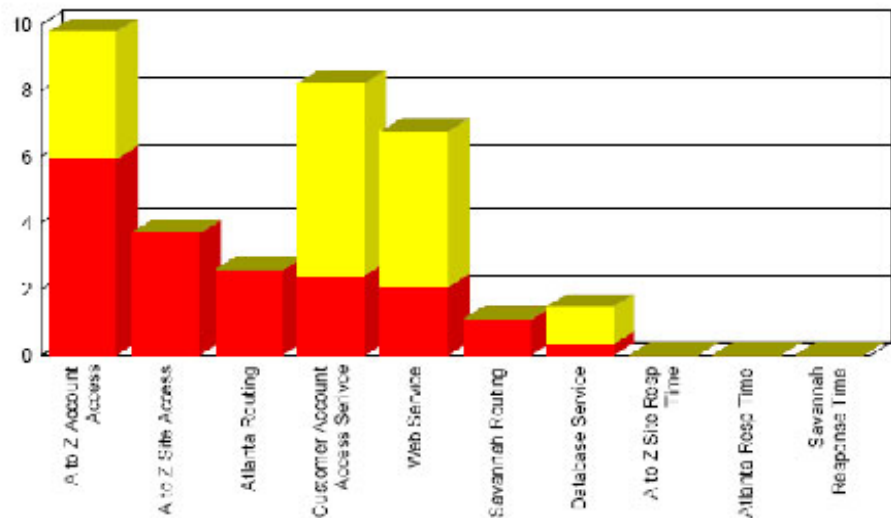
SPECTRUM

Worst Performing Services By Total Outage Time

Date Range: 11/10/2006 12:00:00AM to 11/10/2006 10:14:56AM

Outage Time For Services

In Minutes



Service Name	Up	Down	Degraded	Slightly Degraded
A to Z Account Access				
Percentage	76.37%	14.33%	0.00%	9.30%
Total Time	0 Dy + 10:31:27	0 Dy + 00:05:08	0 Dy + 00:00:00	0 Dy + 00:02:01
Outage Count/MTTR		4 / 0 Dy + 00:01:28	0 / 0 Dy + 00:00:00	2 / 0 Dy + 00:03:31
A to Z Site Access				
Percentage	93.41%	6.66%	0.00%	0.00%
Total Time	0 Dy + 10:52:10	0 Dy + 00:02:12	0 Dy + 00:00:00	0 Dy + 00:00:00
Outage Count/MTTR		3 / 0 Dy + 00:01:14	0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00
Atlanta Routing				
Percentage	98.25%	1.80%	0.00%	0.00%
Total Time	0 Dy + 01:05:53	0 Dy + 00:02:08	0 Dy + 00:00:00	0 Dy + 00:00:00
Outage Count/MTTR		2 / 0 Dy + 00:01:18	0 / 0 Dy + 00:00:00	0 / 0 Dy + 00:00:00

Report Generated 11/10/2006 10:14:56AM

SPECTRUM SERVICE MANAGER

Page 1 of 2

Die Top-N-Services mit der schlechtesten Performance einschließlich der möglichen Ausfallarten

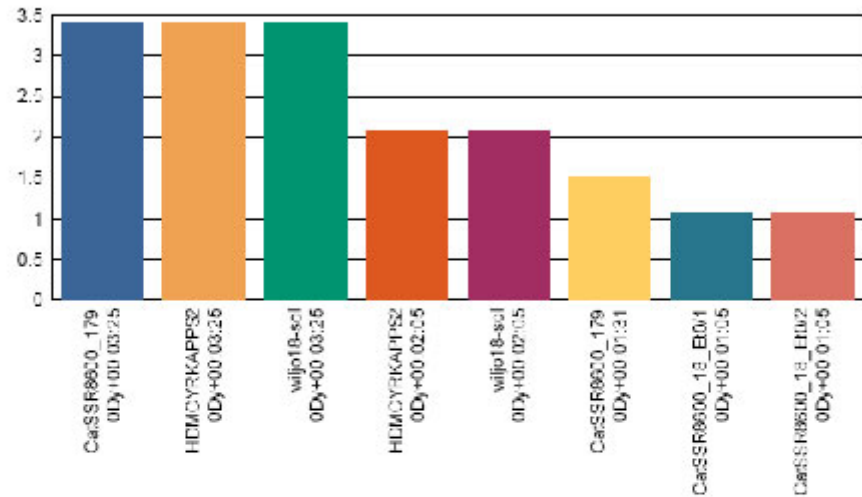
Dieser Bericht weist Ähnlichkeiten mit dem Bericht für Top-N-Services mit der schlechtesten Performance auf, berücksichtigt jedoch neben Ausfallzeiten auch verschlechterte und geringfügig verschlechterte Antwortzeiten. Für jedes Servicemodell sind zusammengefasste Verfügbarkeitsinformationen und Links für detaillierte Serviceverfügbarkeitsberichte verfügbar. Der Bericht enthält sehr detaillierte Informationen für Benutzer von Service Manager, darunter Angaben zu den Services mit den höchsten Gesamtausfallzeiten in einem bestimmten Zeitraum.

Ausfälle bei den Top-N-Services mit der schlechtesten Performance

Mit diesem Bericht können Sie die Ausfälle bei den Top-N-Services mit der schlechtesten Performance anzeigen, die zu Serviceausfallzeiten führten. Dieser Bericht ist ein nützliches Hilfsmittel zur Zusammenfassung der schwerwiegendsten Ausfälle in einem bestimmten Zeitraum, in dem Bereiche in der Servicehierarchie hervorgehoben werden können, die keine Redundanz zum Verhindern von Serviceausfallzeiten aufweisen.

Selected Date Range: 11/10/2006 12:00:00AM to 11/10/2006 10:17:09AM

Worst Resource Outages
In Minutes



Resource	Outage Duration	Impacted Service	Impacted Customers
will018-sol	0 Days + 00:03:25	A to Z Account Access	Customer Information
HDMCYRKAPPS2	0 Days + 00:03:25	A to Z Account Access	Customer Information
CarSR8800_179	0 Days + 00:03:25	A to Z Account Access	Customer Information
will018-sol	0 Days + 00:02:05	Web Service	
will018-sol	0 Days + 00:02:05	Customer Account Access Service	
HDMCYRKAPPS2	0 Days + 00:02:05	Customer Account Access Service	
CarSR8800_179	0 Days + 00:01:31	Atlanta Routing	Customer Information
CarSR8800_179	0 Days + 00:01:31	A to Z Site Access	
CarSR8800_18_B001	0 Days + 00:01:05	A to Z Account Access	Customer Information
CarSR8800_18_B002	0 Days + 00:01:05	A to Z Account Access	Customer Information

Report Generated: 11/10/2006 10:17:09AM

SPECTRUM SERVICE MANAGER

Page: 1

Ressourcen der Top-N-Services mit der schlechtesten Performance nach Gesamtausfallzeit

In diesem Bericht sind zusammengefasste Informationen hinsichtlich der durch einzelne Ressourcen verursachten Gesamtausfallzeit aufgeführt. Dadurch wird die kumulative Wirkung der einzelnen Ressourcenausfälle unterstrichen, die Ausfallzeiten eines oder mehrerer Services nach sich ziehen. Dieser Bericht kann als wichtiges Hilfsmittel zur Identifizierung von Servicere Ressourcen eingesetzt werden, die ständige Problem Bereiche in der Hierarchie der Servicemodellierung darstellen.

Selected Date Range: 11/10/2006 12:00:00AM to 11/10/2006 4:00:10PM

Resource Name	Service Outages	Average Service Outage	Total Service Outage Time	Resource Owner
RK4DCA20	0	0 Days + 01:13:40	0 Days + 09:10:00	0
NT3-RASG-HVNY	6	0 Days + 01:51:40	0 Days + 09:10:00	Rever: Hegel-ek 212-882-7000
wilb1C-sol	3	0 Days + 00:02:31	0 Days + 00:07:36	SNMT Research Inc., #1 (065) 67
NUMUT-RK-1102	8	0 Days + 00:02:01	0 Days + 00:07:36	0
C4ISR8000_172	9	0 Days + 00:02:06	0 Days + 00:06:27	Concord CA Hardware Lab Admin
C4ISR8000_18	9	0 Days + 00:01:11	0 Days + 00:03:39	Concord CA Hardware Lab Admin
C4ISR8000_18_F1001	1	0 Days + 00:01:00	0 Days + 00:01:00	Concord CA Hardware Lab Admin
C4ISR8000_10_C1002	1	0 Days + 00:01:05	0 Days + 00:01:05	Concord CA Hardware Lab Admin
C4ISR8000_18_E1003	1	0 Days + 00:01:06	0 Days + 00:01:06	Concord CA Hardware Lab Admin

Aktueller und letzter SLA-Status nach Kunde

Dieser Bericht stellt eine schnelle Möglichkeit dar, den zusammengefassten SLA-Status für den aktuellen und letzten Zeitraum abzurufen. Dies umfasst nicht betroffene und konforme SLAs sowie SLAs mit Warnstatus und Verletzungen zusammen mit detaillierten Unterberichten, in denen Ergebnisse für bestimmte Gewährleistungen aufgeführt sind. Dieser Bericht kann für ausgewählte SLAs oder für SLAs für einen bestimmten Kunden ausgeführt werden. Mit diesem Bericht kann schnell ein Überblick über den Status verschiedener SLAs für beliebig viele Kunden bereitgestellt werden.

Report Generated: 11/10/2006 4:12:34PM

Service Level Agreement	Period	Status	Customer
A to Z Customer Account Access SLA	Nov 10 - Nov 11, 2006	Warning	A to Z Performance Components
A to Z Billing Service SLA	Nov 1 - Dec 1, 2006	Unaffected	A to Z Performance Components
BW Tech Provisioning SLA	Nov 1 - Dec 1, 2006	Unaffected	BW TECH
BW Tech Customer Account Access SLA	Nov 1 - Dec 1, 2006	Unaffected	BW TECH

SLA-Zusammenfassung nach: Name, Kunde, Status

Dieser Bericht enthält eine Tabelle zusammengefasster SLA-Statuswerte für einen oder mehrere Zeiträume. Der Bericht kann nach SLA-Name oder Kundenname erstellt oder einfach nach Statuswerten unterteilt werden. Er kann als zusammengefasste Referenz für mehrere SLAs oder mehrere Zeiträume verwendet werden. Sie können auf detaillierte Unterberichte mit Ergebnissen für bestimmte Gewährleistungen zugreifen.

Date Range: 11/10/2006 12:00:00AM to 11/10/2006 4:14:18PM

A to Z Performance Components				
Status	SLA Name	SLA Period Start	SLA Period End	Period Details
Compliant	A to Z Customer Account Access SLA	11/10/2006 8:52:21AM	11/11/2006 5:00:00AM	Period Details
Compliant	A to Z Billing Service SLA	11/11/2006 6:00:00AM	12/1/2006 6:00:00AM	Period Details

BW TECH				
Status	SLA Name	SLA Period Start	SLA Period End	Period Details
Compliant	BW Tech Provisioning SLA	11/11/2006 5:00:00AM	12/1/2006 5:00:00AM	Period Details
Compliant	BW Tech Customer Account Access SLA	11/11/2006 5:00:00AM	12/1/2006 5:00:00AM	Period Details

SLA-Zusammenfassung: Warnung oder Verletzung

Dieser Bericht enthält eine Tabelle aller SLAs, die derzeit einen Warnstatus oder eine Verletzung aufweisen. Über die Tabelle können Sie zudem auf einen Unterbericht zugreifen, in dem detaillierte Informationen zu den Ausfällen einer bestimmten Gewährleistung im aktuellen Zeitraum aufgeführt sind. Dies ist ein nützlicher Bericht für Benutzer von Service Manager, um SLAs anzuzeigen, deren Performance im aktuellen Zeitraum beeinträchtigt ist.

Report Time: 11/10/2006 4:16:33PM

SLA Periods With Status: Compliant - Warned					
Status	SLA Name	SLA Period Start	SLA Period End	Period Details	Customer
Warned	A to Z Customer Account Access SLA	11/10/2006 8:52AM	11/11/2006 5:00AM	Period Details	A to Z Performance

SLA-Details nach: SLA-Name, Zeitbereich, n letzte Perioden

Dieser Bericht ähnelt dem Bericht für SLA-Details nach Kunden, enthält jedoch alle SLA-Statuswerte, einschließlich nicht betroffener und konformer Status sowie Warn- und Verletzungsstatus. In einem Unterbericht sind detaillierte Informationen aufgeführt, darunter Gewährleistungsausfälle für den entsprechenden Zeitraum. Dies ist hilfreich zum Abrufen ausführlicher Informationen zu einzelnen SLAs in einem oder mehreren Zeiträumen.

SPECTRUM

Service Level Agreement Detail Report

Date Range: 11/10/2006 12:00:00AM to 11/10/2006 10:24:30AM

A to Z Customer Account Access SLA			
Guarantees Customer Account Access Service Service Customer Information for A to Z Performance Components Description: SLA for A to Z Performance Components provided by North East Data Solutions.		Guarantee Status Distribution Unaffected Compliant Warned Violated	
Customer Access Availability - Monitors Customer Account Access Service Service		Availability Report	
	Compliant - (Affected)	Nov 10, 2006 - Nov 11, 2006	Period Details
Cust Access Business Hours Availability - Monitors Customer Account Access Service Service		Availability Report	
	Compliant - (Affected)	Nov 10, 2006 - Nov 11, 2006	Period Details
Atlanta Routing 7x24 Availability - Monitors Atlanta Routing Service		Availability Report	
	Compliant - (Warned)	Nov 10, 2006 - Nov 11, 2006	Period Details
Atlanta Routing Business Hours Availability - Monitors Atlanta Routing Service		Availability Report	
	Compliant - (Unaffected)	Nov 10, 2006 - Nov 11, 2006	Period Details
Savannah Router 7x24 Availability - Monitors Savannah Routing Service		Availability Report	
	Compliant - (Affected)	Nov 10, 2006 - Nov 11, 2006	Period Details
Savannah Routing Business Hours Availability - Monitors Savannah Routing Service		Availability Report	
	Compliant - (Affected)	Nov 10, 2006 - Nov 11, 2006	Period Details
Atlanta RespTime Time Business Hours Availability - Monitors Atlanta Resp Time Service		Availability Report	
	Compliant - (Unaffected)	Nov 10, 2006 - Nov 11, 2006	Period Details
Savannah Resp Time Business Hours Availability - Monitors Savannah Response Time Service		Availability Report	
	Compliant - (Unaffected)	Nov 10, 2006 - Nov 11, 2006	Period Details

Report Generated 11/10/2006 at 10:24:31AM

SPECTRUM SERVICE MANAGER

Page 1 of 2

UNTERBERICHTE MIT ZEITRAUMDETAILS

Guarantee Detail Report

SPECTRUM

Period Start: 11/10/2006 5:00:00AM
 Period End: 11/11/2006 5:00:00AM
 Activation Time: 11/10/2006 9:52:21AM

Arlanta Routing 7x24 Availability

Compliant - (Warned)

Guarantee Configuration

Guarantees 99.00 Availability

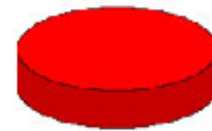
Warning Threshold: 0 Days + 00:11:31 or 80.00% of violation threshold

Violation Threshold: 0 Days + 00:14:24

Period Performance

Statistic	Status	Threshold	Value
DOWNTIME	Compliant	0 Days + 00:14:24	0 Days + 00:02:36
MDT	Disabled	0 Days + 00:00:00	0 Days + 00:01:31
MTTR	Compliant	0 Days + 00:30:00	0 Days + 00:01:18
MTBF	At Risk	1 Day + 00:00:00	0 Days + 00:01:27

Summary of Outages



Unplanned
 Planned
 Exempt

Related Incidents

Start Time	End Time	Outage Duration	Outage Time This Period	Incident Status
Fri 11/10/06 10:07:29	Fri 11/10/06 10:09:20	0 Days +00:01:31	0 Days + 00:01:31	Unplanned
Fri 11/10/06 10:17:07	Fri 11/10/06 10:11:12	0 Days +00:01:05	0 Days + 00:01:05	Unplanned
			0 Days + 00:02:36	

* Indicates outage is ongoing

| Indicates time adjusted for period

Report Generated: 11/10/2006 at 10:54:51AM

SPECTRUM SERVICE MANAGER

Page 1 of 1

Guarantee Detail Report

SPECTRUM

Period Start: 11/10/2006 00:00:00AM
 Period End: 11/11/2006 5:00:00AM
 Activation Time: 11/10/2006 8:02:10AM

Savannah Routing Business Hours Availability

Compliant - (Affected)

Guarantee Configuration

Guarantee: 99.50 Availability

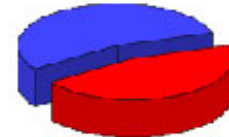
Warning Threshold: 0 Days + 00:05:45 or 00.00% of violation threshold

Violation Threshold: 0 Days + 00:07:12

Period Performance

Statistic	Status	Threshold	Value
DOWNTIME	Compliant	0 Days + 00:07:12	0 Days + 00:01:20
MOT	Compliant	0 Days + 00:20:00	0 Days + 00:01:20
MTTR	Disabled	0 Days + 00:00:00	0 Days + 00:01:30
MTBF	Disabled	0 Days + 00:00:00	0 Days + 00:00:30

Summary of Outages



Unplanned
 Planned
 Exempt

Related Incidents

Start Time	End Time	Outage Duration	Outage Time (Inc Period)	Incident Status
En 11/10/06 10:12:14	En 11/10/06 10:13:20	0 Days +00:01:06	0 Days + 00:01:06	Unplanned
En 11/10/06 10:20:10	En 11/10/06 10:21:30	0 Days +00:01:20	0 Days + 00:01:20	Exempt

Notes: Power failure at Savannah location. [root]

0 Days + 00:01:26

* Indicates outage is ongoing

† Incidents time adjusted for period

Report Generated 11/10/2006 at 10:24:31AM

SPECTRUM SERVICE MANAGER

Page 1 of 1

SLA-Details mit Ressourcenausfällen

In diesem komplexen Bericht sind SLA-Status und die zugeordneten Ressourcenausfälle zusammen aufgeführt, die sich letztendlich in einem bestimmten Zeitraum auf das SLA ausgewirkt haben. Dieser Bericht ist von Nutzen, wenn er in Verbindung mit dem Bericht für Ressourcen der Top-N-Services mit der schlechtesten Performance nach Gesamtausfallzeit verwendet wird. Mit Hilfe dieses Berichts können Sie die Wirkung einer bestimmten Ressource auf oberster Ebene anzeigen. Da er eine große Anzahl Informationen enthält, werden bei SLAs mit zahlreichen Ressourcenausfällen möglicherweise viele Datenseiten erstellt.


SLA Resource Outage Report

Date Range: November 10, 2008 to November 11, 2008


A to Z Customer Account Access SLA
Period: November 10, 2008 to November 11, 2008
Status for period: Compliant - (Warned)

Description: SLA for A to Z Performance Components provided by North East Data Solutions.

[Customer Information For A to Z Performance Components](#)


Savannah Business Hours Response Time Guarantee Compliant - (Unaffected)
[Period Details](#)

Statistic	Status	Threshold	Actual
Required Time	Compliant	0 Days + 01:10:00	0 Days + 01:10:00


Atlanta Business Hours Response Time Guarantee Compliant - (Unaffected)
[Period Details](#)

Statistic	Status	Threshold	Actual
Required Time	Compliant	0 Days + 01:10:00	0 Days + 01:10:00


Savannah Resp Time Business Hours Availability Guarantee Compliant - (Unaffected)
[Period Details](#)

Statistic	Status	Threshold	Actual
Down Time	Compliant	0 Days + 00:14:24	0 Days + 00:00:00
Maximum Outage Time	Compliant	0 Days + 00:20:00	0 Days + 00:00:00


Atlanta RespTime Time Business Hours Availability Guarantee Compliant - (Unaffected)
[Period Details](#)

Statistic	Status	Threshold	Actual
Down Time	Compliant	0 Days + 00:14:24	0 Days + 00:00:00
Maximum Outage Time	Compliant	0 Days + 00:20:00	0 Days + 00:00:00


Savannah Routing Business Hours Availability Guaranteed Compliant - (Affected)
[Period Details](#)

Statistic	Status	Threshold	Actual
Down Time	Compliant	0 Days + 00:07:12	0 Days + 00:01:06
Maximum Outage Time	Compliant	0 Days + 00:20:00	0 Days + 00:01:06

Resource outages impacting Savannah Routing Service

Duration = 0 Days + 00:04:20 From: 11/10/2008 10:20:10AM To: 11/10/2008 10:21:30AM (Exempt)
Cat5 SR6500_16 - Unable to contact device

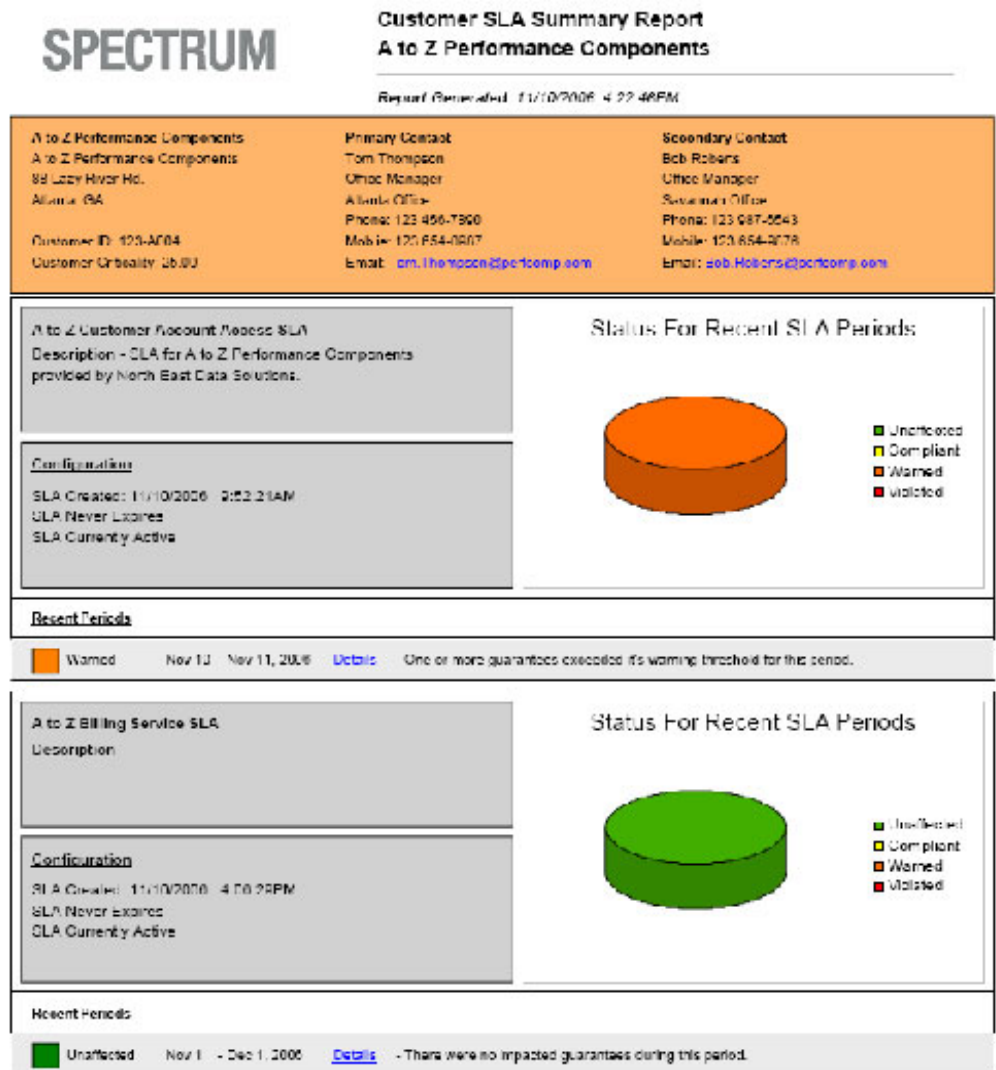
Report Generated: 11/10/2008 4:49:12PM

SPECTRUM SERVICE MANAGER

Page 1 of 3

Kundenspezifische SLA-Zusammenfassung

In diesem Bericht ist der Status der letzten sechs SLA-Zeiträume für alle SLAs eines Kunden aufgeführt. Der Status umfasst alle vier Werte. Für jedes SLA wird ein Diagramm mit einer Zusammenfassung der Statusinformationen aller sechs Zeiträume in einer Tabelle dargestellt, in der die Daten für jeden Zeitraum sowie ein Link für detaillierte Informationen zu den Ausfällen der Gewährleistungen aufgeführt sind. Mit diesem Bericht können Servicemanager schnell die SLA-Performance für einen bestimmten Kunden in den jeweils letzten sechs Zeiträumen anzeigen. Der Bericht kann zudem von der Vertriebsabteilung eingesetzt werden, um zu prüfen, ob die SLAs eines Kunden in den letzten Zeiträumen eingehalten wurden.



(Diese Seite wurde absichtlich leer gelassen)

Kapitel 8: Proaktive Servicesicherung

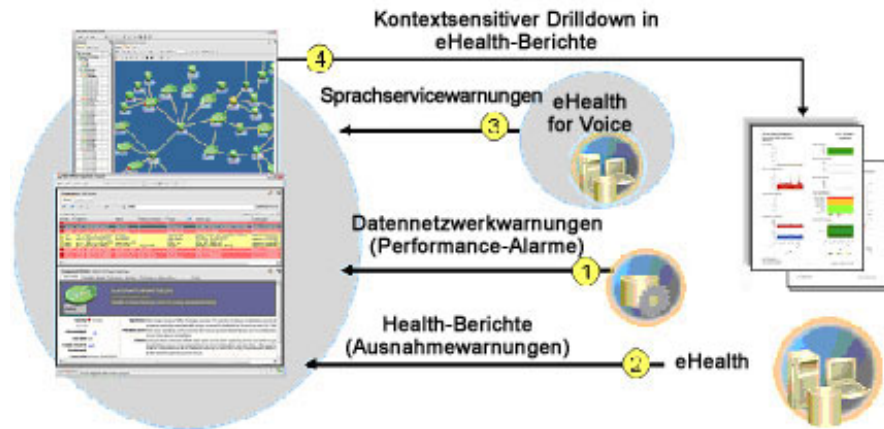
Die CA-Lösung für Netzwerk- und Sprachmanagement verfügt über integrierte Algorithmen, mit deren Hilfe Netzwerkteams wachsende Problembereiche in der Infrastruktur erkennen können, **bevor** sich diese auf den Kundenservice auswirken. Probleme treten in den seltensten Fällen unmittelbar auf. Häufig weisen Warnsignale auf geringfügige, jedoch wachsende Serviceverschlechterungen, zunehmende Fehler und Verzögerungen hin. Diese Probleme sind unter Umständen nicht so gravierend, dass Benutzer sie bemerken oder dass sie Serviceanrufe rechtfertigen, sie wachsen jedoch zunehmend.

Mit Tools, mit denen wachsende Probleme analysiert und erkannt sowie Warnungen ausgegeben werden können, können Netzwerkteams die Probleme proaktiv beheben, bevor diese zu Ausfällen und Serviceunterbrechungen oder -ausfällen führen. Diese Funktionen sind vor allem bei der SLA-Umsetzung von großer Bedeutung. Wenn Sie SLA-Probleme vor der Verletzung des entsprechenden SLA ohne zusätzliche Netzwerkressourcen und Netzwerkservers lösen können, können Sie übermäßigen Aufwand und überhöhte Kosten vermeiden.

Voraussetzungen: Bei den Verfahren in diesem Kapitel wird vorausgesetzt, dass SPECTRUM und eHealth installiert sind und dass Live Health so konfiguriert wurde, dass Traps an SPECTRUM gesendet werden können. Weitere Informationen zur Konfiguration der integrierten Produktlösung finden Sie in Kapitel 5. Ausführliche Informationen zur Anwendung Live Health und zum Erstellen von Überwachungsregeln finden Sie in der Webhilfe zu Live Health. Die Webhilfe zu eHealth ist auf dem eHealth-System installiert und zudem auf der CD mit der Online-Dokumentation für TotalDoc verfügbar.

Identifizierung potenzieller Probleme

Die proaktive Analyse der Anwendung eHealth Live Health und die Ausnahmeanalyse der Health-Berichte sind die Haupttools, mit denen Sie vor wachsenden Netzwerkproblemen gewarnt werden. Bei konvergenten Netzwerken werden beginnende Sprach- und Messaging-Probleme mit Hilfe von eHealth for Voice Policy Manager erkannt. Alle diese Tools enthalten konfigurierbare Schwellenwerte und Einstellungen, so dass Sie definieren können, zu welchem Zeitpunkt ein Problem so schwerwiegend ist, dass proaktive Maßnahmen angemessen sind.



Sie können diese Tools so konfigurieren, dass die wachsenden Probleme automatisch überwacht werden und Alarme an SPECTRUM gesendet werden, wenn hinsichtlich der Probleme Maßnahmen ergriffen werden müssen. Darüber hinaus können Sie die Zeitdauer für das entsprechende Verhalten festlegen, nach der Alarme ausgelöst werden, so dass „falsche“ Alarme bei einfachen Schwellenwertüberschreitungen reduziert werden und die realen, wachsenden Problemfälle im Mittelpunkt stehen.

Mit der Anwendung Live Exceptions der Live Health-Produktfamilie werden beispielsweise Benachrichtigungen bei potenziellen Verzögerungen, Fehlern und ungewöhnlichen Auslastungsproblemen in Netzwerken, Systemen und Anwendungen bereitgestellt. Dabei werden anhand der mit eHealth erfassten und verwalteten Verlaufsdaten potenzielle Probleme festgestellt. Wenn mit Hilfe von Live Exceptions eine Bedingung ermittelt wird, bei der der Bediener eingreifen müssen, wird ein Alarm ausgelöst und an SPECTRUM gesendet.

Konfiguration von Live Health zur Beobachtung wachsender Probleme

Zur proaktiven Servicesicherung können Sie über die Algorithmen bei zeitlicher Überschreitung von Schwellenwerten und bei Normabweichungen in Live Exceptions die wachsenden Serviceprobleme überwachen. Wenn die Performance (entsprechend vergangener Erfahrungen) für eine bestimmte Zeitdauer vom Normalverhalten abweicht, wird in Live Health ein Alarm ausgelöst und an SPECTRUM gesendet.

So konfigurieren Sie Live Health für die proaktive Servicesicherung:

1. Ordnen Sie über den Live Exceptions-Browser die entsprechenden Standardprofile vom Typ „Unusual Workload“ zu Gruppen oder Gruppenlisten der verwalteten Ressourcen zu. Verwenden Sie das Live Health Profile Descriptions Tool unter <http://support.concord.com/devices> zur Identifizierung der korrekten Profile für die erkannten Elementtypen. Weitere Informationen zum Zuordnen von Profilen zu Gruppen finden Sie in Kapitel 5.
2. Bei benutzerdefinierten SLAs können Sie benutzerdefinierte Profile mit Alarmen bei zeitlicher Überschreitung von Schwellenwerten und Alarmen bei Normabweichungen verwenden, die Serviceschwellenwerte darstellen. Stellen Sie sicher, dass die Regeln so konfiguriert sind, dass Warnungen erzeugt werden, wenn bei Serviceverschlechterungen Maßnahmen ergriffen werden müssen, typischerweise bei einem Schwellenwert, der unterhalb der Schwellenwerte des Service-Agreement liegt. Anweisungen zum Erstellen benutzerdefinierter Profile finden Sie in der Webhilfe zu Live Health.

Konfiguration von Health-Berichten zum Senden von Traps bei wachsenden Problemen

Der Ausnahmebereich eines Health-Berichts enthält Informationen zu Elementen, bei denen ungewöhnliche Ereignisse eingetreten sind oder die möglicherweise keine ausreichenden Ressourcen für den entsprechenden Bedarf aufweisen. In diesem Bereich eines Health-Berichts werden Elemente angezeigt, bei denen aufgrund von Fehlern, hoher Auslastung und Trendabweichungen eine hohe Anzahl von Ausnahmepunkten angefallen ist. Elemente sind im Bericht nur aufgeführt, wenn die akkumulierten Ausnahmepunkte eine Mindestanzahl überschreiten. Administratoren von eHealth können diese Anzahl im Serviceprofil des Berichts angeben.

Als zusätzliches Hilfsmittel für die proaktive Serviceüberwachung können Sie Health-Berichte so konfigurieren, dass Traps für Health-Ausnahmen an SpectroSERVER weitergeleitet werden. Wenn der geplante Health-Bericht ausgeführt wird, wird in eHealth für das höchstrangige Problem jedes Elements, das im Ausnahmebereich des Health-Berichts aufgeführt ist, ein SNMP-Trap an SpectroSERVER gesendet. Die Weiterleitung von Traps ist in der Standardeinstellung für eHealth nicht aktiviert. Sie müssen einen benutzerdefinierten Health-Bericht erstellen, um diese Funktion zu aktivieren, und dann diesen Health-Bericht so planen, dass er automatisch ausgeführt wird.

Hinweis: Ausnahmen können nur von geplanten Health-Berichten weitergeleitet werden. Bei der manuellen Ausführung von Health-Berichten werden keine Ausnahmen weitergeleitet.

Anweisungen zum Erstellen eines benutzerdefinierten Health-Berichts, mit dem Ausnahmen als Traps an Live Health weitergeleitet werden, finden Sie in Kapitel 5.

Senden von Sprach-Alerts an SPECTRUM

eHealth for Voice 4.0 bietet Alarmintegration und -korrelation mit SPECTRUM. Dazu werden die SPECTRUM-Funktionen für Servicemanagement und Sprachmodellierung eingesetzt. Sie können die Anwendung eHealth for Voice Policy Manager so konfigurieren, dass SNMP-Traps an SPECTRUM gesendet werden, wenn QoS- oder GoS-Verletzungen auftreten. In SPECTRUM wird anhand der Informationen zu Richtlinien, Modellen und Regeln der Schweregrad des Problems ermittelt.

Mit Policy Manager werden alle Daten-, Sprach- und PBX-Aktivitäten überwacht und anschließend anhand vordefinierter Kriterien geprüft. Mit Hilfe von Policy Manager können Sie Regeln oder Richtlinien für beliebige Daten festlegen, z. B. Konfigurationsänderungen, Systemdatenverkehr, Einzelauslastung, Alarme oder Verlaufereignisse. Anweisungen zur Konfiguration von eHealth for Voice zum Senden von Performance-Traps an SPECTRUM finden Sie in Kapitel 5.

Reaktion auf Alarmaktionen in SPECTRUM

Über die SPECTRUM OneClick-Konsole können Netzwerkbetreiber und -manager die Modelle (oder Ressourcen) in der entsprechenden Topologie anzeigen sowie Ereignisse oder Statusänderungen überwachen, die auf wachsende Probleme im Netzwerk hinweisen. Wenn in SPECTRUM ein Trap von eHealth empfangen wird, ändert sich die Farbe des Modells, das das Element darstellt, so dass der Schweregrad des Alarms des empfangenen Traps angegeben wird. Wenn schwerwiegende Probleme auftreten, wird das entsprechende Gerätesymbol beispielsweise rot angezeigt, während es bei geringfügigen Problemen gelb angezeigt wird.

Bediener können mit der rechten Maustaste auf das Symbol klicken und folgende Vorgänge durchführen, um die Probleme zu beheben oder zu überprüfen:

- Navigieren zu einem eHealth-Alarmdetailbericht, um die Performance-Trends anzuzeigen, aufgrund derer in Live Health Leistungsprobleme erkannt wurden und ein Alarm ausgelöst werden musste. Wenn ein Gerät beispielsweise länger als 15 Minuten außerhalb des normalen Betriebsschwellenwerts betrieben wurde, können Sie in den Live Health-Alarmdetailberichten die Performance-Trends für dieses Element anzeigen.
- Ausführen eines Übersichts- oder Trend-Berichts in eHealth, um den Leistungsverlauf der Ressource zu prüfen. In einem Trend-Bericht ist die Performance der betreffenden Problemvariablen aufgeführt, in einem Übersichtsbericht dagegen eine Gruppe allgemeiner Performancevariablen für den entsprechenden Elementtyp. Anhand dieser Daten können Sie beitragende Gründe oder die Ursache des Problems ermitteln.
- Löschen des Alarms. Wenn der Bediener weiß, dass sich der Alarm auf bekannte Probleme oder Fälle bezieht, kann er den Alarm löschen und den Gerätestatus auf den normalen Status zurücksetzen.
- Öffnen von Service Desk-Tickets, um das Problem als Arbeitsaufgabe zu erfassen und zum Beheben bestimmten Mitarbeitern zuzuweisen. Durch die Integration in Unicenter Service Desk können Service Desk-Tickets, mit denen Aufgaben zum Beheben von Problemen im Netzwerk nachverfolgt werden, in SPECTRUM geöffnet, geändert und geschlossen werden. Bediener können über die OneClick-Konsole zu den Details zu Service Desk-Tickets navigieren, um den neuesten Status der Tickets und die jeweils für die Problembehebung zugewiesenen Mitarbeiter zu ermitteln.

Kapitel 9: Vorausschauende Kapazitätsplanung

Sowohl die Arbeitseffizienz als auch die Kundenzufriedenheit hängen von der Verfügbarkeit und Performance geschäftskritischer Anwendungen ab. Die Anwendungen sind an die fehlerfreie und effiziente Ausführung der IT-Infrastruktur gebunden.

Zur Gewährleistung, dass IT-Ressourcen die Anforderungen der Benutzer erfüllen, bedarf es mehr als der bloßen Reaktion auf Probleme. Wenn die Infrastruktur effizient ausgeführt werden soll, müssen Sie Echtzeitdaten zum aktuellen Status des Netzwerks abrufen, Überlastungs- und Problembereiche erkennen, bevor sich diese auf Benutzer auswirken, sowie effektive Planungen für die Zukunft festlegen. Alle diese Aufgaben sind Bestandteil der vorausschauenden Kapazitätsplanung.

Die Kapazitätsplanung ist ein komplexer und wichtiger Bestandteil der Verwaltung von IT-Ressourcen. Mit Hilfe der Kapazitätsplanung können Sie die aktuellen Ressourcen effizient einsetzen, Bedarfstrends ermitteln und zukünftige Ressourcenanforderungen herausarbeiten. Durch eine effektive Kapazitätsplanung können Sie Folgendes erreichen:

- Verringern von Kosten durch Reduzierung oder Eliminierung unterbeanspruchter Mietleitungen
- Verbessern der Performance durch Bestimmung der über- und unterbeanspruchten Elemente sowie durch Anpassen der Kapazität an den Bedarf
- Verringern von Server- und Netzwerkausfallzeiten durch Erkennung von Überlastungen vor deren Auftreten und durch Prüfen der entsprechenden Kapazitäten
- Verbessern der Budgetvorhersagbarkeit durch Nachverfolgen von Trends und Modellieren der Auswirkungen neuer Services oder Infrastrukturen zur Vermeidung von Notkäufen und Sicherstellung der günstigsten Preise

In diesem Kapitel wird beschrieben, wie Sie mit Hilfe von eHealth drei Hauptaufgaben der Kapazitätsplanung ausführen können:

- Erkennen unterbeanspruchter Ressourcen zum Suchen vorhandener Geräte oder Ressourcen, die unzureichend ausgelastet sind, was zu unnötigen Kosten für Mietleitungen und zu Systemen im Leerlauf führt
- Identifizieren überbeanspruchter Ressourcen zum Suchen vorhandener Geräte oder Ressourcen, die übermäßig ausgelastet sind, was zur Verschlechterung der Performance oder zu Einbußen aufgrund von Überbelastung führt
- Planen zukünftiger Kapazitätsanforderungen anhand aktueller Bedarfstrends oder voraussichtlicher Unternehmensänderungen, so dass Sie Käufe planen und bei Bedarf Aktualisierungen installieren können
- Durchführen der Planung von Sprachkapazitäten zur Suche von Problemen aufgrund von Unter- oder Überbelastung in Telco-Netzwerken oder konvergenten Netzwerken

Voraussetzungen: Zur Verwendung der Best Practices in diesem Kapitel müssen in der eHealth-Datenbank mindestens eine Woche lang Daten erfasst worden sein. Die Effektivität dieser Berichte erhöht sich hinsichtlich der Hervorhebung von Kapazitätstrends und Auslastungsproblemen durch eine höhere Anzahl von Performance-Daten und Verlaufsdaten.

Bei diesen Beispielen wird zudem davon ausgegangen, dass die Berichte über die eHealth-Weboberfläche angezeigt werden. Die Berichte auf der Weboberfläche verfügen über interaktive „Hotspots“, auf die Sie klicken können, um zu anderen Berichten und ausführlichen Daten zu navigieren. In Berichten im PDF-Format ist keine Navigation möglich.

Weitere Referenzquellen: Die Verfahren zum Ausführen, Planen und Anpassen von Berichten werden im *eHealth Report Management Guide* und in der Webhilfe zu eHealth ausführlich erläutert. Detaillierte Informationen zu eHealth-Berichten und deren Verwendung finden Sie in der Webhilfe zu eHealth. Die Best Practices in diesem Abschnitt stammen aus dem Thema *Capacity Planning with eHealth*, das Sie auf der eHealth-Supportwebsite unter <http://support.concord.com> finden.

Identifizierung von nicht ausgelasteten Ressourcen

Führen Sie folgende Schritte aus, um nicht ausgelastete Ressourcen zu ermitteln:

1. Suchen der nicht ausgelasteten Ressourcen
2. Bestätigen der unzureichenden Auslastung
3. Beheben der unzureichenden Auslastung der Ressourcen
4. Anzeigen des ROI
5. Aktualisieren der Konfiguration

Lokalisierung von nicht ausgelasteten Ressourcen

eHealth enthält einen Bericht zu unterbeanspruchten Elementen, mit dem Sie schnell Elemente identifizieren können, die möglicherweise unzureichend ausgelastet sind. Dieser Bericht ist ein optionaler Zusatzbericht der Health-Berichte in eHealth. Wenn Sie diesen Bericht anzeigen möchten, müssen Sie einen Health-Bericht so anpassen, dass er diesen Zusatzbericht enthält.

So suchen Sie die unterbeanspruchten Elemente im Netzwerk:

1. Melden Sie sich auf der eHealth-Weboberfläche an, und klicken Sie auf die Registerkarte „Run Reports“.
2. Klicken Sie auf den Link für den Health-Standardbericht. Daraufhin wird die Seite „Run Health Report“ angezeigt.
3. Geben Sie die Berichtsmerkmale an, z. B. LAN/WAN-Technologie und eine Elementgruppe.
4. Klicken Sie auf „More Options“, und wählen Sie unter „Presentation Attributes“ die Option „Supplemental“ aus.
5. Wählen Sie in der Liste der Berichte vom Typ „Supplemental“ den Eintrag „Underutilized Elements“ aus, so dass dieser Bericht einbezogen wird.
6. Speichern Sie den Bericht mit einem eindeutigen Namen, z. B. Underutilization_Report.

7. Klicken Sie auf „Generate Report“, um den Bericht auszuführen. Da die Ausführung des Berichts mehrere Minuten in Anspruch nehmen kann, empfiehlt es sich, den Bericht über die eHealth-Konsole auszuführen, so dass er über Nacht oder zu einem Zeitpunkt ausgeführt wird, zu dem das eHealth-System nicht ausgelastet ist.
8. Prüfen Sie den Zusatzbericht zu unterbeanspruchten Elementen. In dem Bericht sind die Elemente aufgeführt, die in den vergangenen 8 Tagen folgende Kriterien erfüllt haben:
 - > Die zu keinem Zeitpunkt eine Auslastung von 50 % erreicht haben
 - > Die über 5 % der Zeit keine Auslastung von 10 % erreicht haben
9. Suchen Sie in dem Bericht nach Mietleitungen, Routern, Switches und Systemen, deren Bandbreite, CPU-Kapazität, Arbeits- oder Festplattenspeicher unzureichend ausgelastet sind. Im folgenden Bericht werden z. B. mehrere OC-3-Hochgeschwindigkeitsleitungen aufgelistet, die über eine sehr geringe Auslastung verfügen und daher genauer analysiert werden sollten.

Underutilized Elements

			Element	
Rank	Element Name	Speed	Type	Utilization Exception
1	helium:-5734-ATM2/0	156.2 Mbs	ATM WAN Port	Underutilized Link, 99.00% of the baseline below 10% utilization (In)
2	helium:-5734-ATM2/0	156.2 Mbs	ATM WAN Port	Underutilized Link, 99.00% of the baseline below 10% utilization (Out)
3	helium:-5734-ATM3/0	156.2 Mbs	ATM WAN Port	Underutilized Link, 99.00% of the baseline below 10% utilization (In)
4	helium:-5734-LEC.1.13	156.2 Mbs	Generic LAN Interface	Underutilized Link, 99.00% of the baseline below 10% utilization (In)
5	helium:-5734-LEC.1.13	156.2 Mbs	Generic LAN Interface	Underutilized Link, 99.00% of the baseline below 10% utilization (Out)
6	helium:-7839-ATM0/0	155.5 Mbs	Generic WAN Interface	Underutilized Link, 99.00% of the baseline below 10% utilization (In)

Wenn Sie den Bericht zu unterbeanspruchten Elementen nur für LAN- bzw. WAN-Elemente ausführen, werden diese zunächst nach der Geschwindigkeit (aufgrund der höheren Kosten für WAN-Verbindungen) und erst dann nach der Zeitdauer (in Prozent) sortiert, für die die Elemente nicht ausgelastet waren.

BEST PRACTICES

Für den Bericht zu unterbeanspruchten Elementen empfehlen sich folgende Best Practices, um genauere Aussagen zur Umgebung zu treffen:

- Wenn Sie eHealth erstmalig installieren, sollten Sie es in wöchentlichen Abständen ausführen, um nicht verwendete Ressourcen zu identifizieren. Nach dieser Anfangsphase können Sie die Abstände (monatlich oder vierteljährlich) vergrößern, um Änderungen in der Nutzung des Netzwerks zu ermitteln.
- Da in dem Bericht zu unterbeanspruchten Elementen Daten aus den vergangenen 8 Tagen berücksichtigt werden, sollten Sie die Ausführung des Berichts für den Sonntag einplanen. Auf diese Weise werden die Daten der gesamten Geschäftswoche ausgewertet.
- Je nach Nutzung des Netzwerks können Sie das Serviceprofil so bearbeiten, dass nur die Daten von bestimmten Tagen oder Zeiten in den Bericht aufgenommen werden, während

Zeiten mit geringer Netzwerkauslastung, z. B. Nächte oder Wochenenden, von vornherein ausgeschlossen werden.

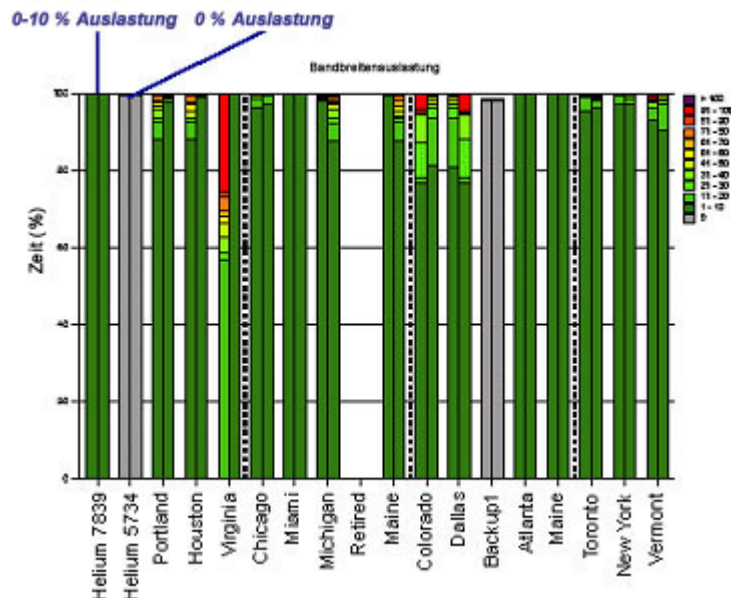
Bestätigung der unzureichenden Auslastung

Nachdem Sie die unterbeanspruchten Elemente ermittelt haben, analysieren Sie deren Funktion, und führen Sie entsprechende Berichte aus, um sich zu vergewissern, dass die Elemente tatsächlich unzureichend ausgelastet sind. Führen Sie einen monatlichen Health-Bericht aus, um sich zu vergewissern, dass das Netzwerk für mindestens einen Monat nicht genügend beansprucht wurde.

Wichtig: Überprüfen Sie die nicht ausgelasteten Netzwerkverknüpfungen, um zu ermitteln, ob es sich um Sicherungen handelt. Da Sicherungen nur dann verwendet werden, wenn die primären Systeme ausfallen, werden die Sicherungen häufig überhaupt nicht beansprucht.

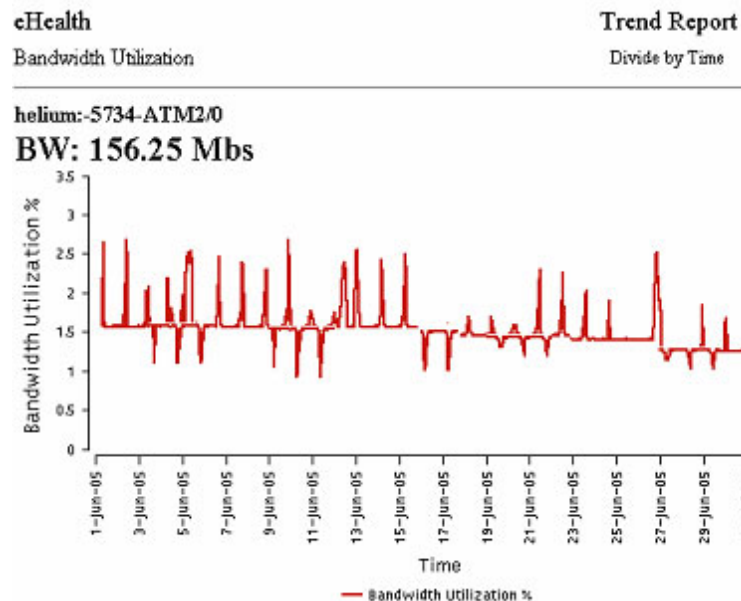
So überprüfen Sie, ob ein Element nicht ausgelastet ist:

1. Öffnen Sie den Health-Bericht (z. B. den aus dem letzten Abschnitt), und analysieren Sie auf der Seite mit den Elementdetails das Diagramm zur Bandbreitennutzung.



Das Diagramm zur Bandbreitennutzung gibt an, wie die einzelnen Netzwerkinterfaces während des Berichtszeitraums ausgelastet wurden. Der Balken von Helium 5734 ist beispielsweise vollständig grau, was darauf hindeutet, dass das Element während dieses Monats überhaupt nicht beansprucht wurde. Diverse andere Balken, wie die von Helium 7839, Miami und Atlanta, sind dunkelgrün dargestellt, was darauf hindeutet, dass die Auslastung zu keinem Zeitpunkt über 10 % lag. Alle diese Interfaces werden nur unzureichend ausgelastet.

- Führen Sie den Bandbreitentrend-Bericht aus, indem Sie auf den Balken des Elements klicken, von dem Sie annehmen, dass es nicht ausgelastet ist. Im Bandbreitentrend-Bericht wird die Auslastung des Elements für den gleichen Zeitraum angezeigt wie im Health-Bericht.



- Überprüfen Sie, ob das Netzwerk infolge einer Neukonfiguration entweder permanent unausgelastet ist oder ob plötzliche Abfälle in der Nutzung auftreten. Das Element im obigen Beispiel erreicht z. B. während des gesamten Monats keine Auslastung von über 3,5 %, was darauf hindeutet, dass das Element nicht ausgelastet ist.
- Erstellen Sie einen Berichtsverlauf, um die Hinweise auf die geringe Auslastung zu dokumentieren. Neben den wöchentlichen und monatlichen Health-Berichten können Sie einen Service-Level-Bericht für Servicekunden ausführen, in dem die Bandbreitennutzung über einen längeren Zeitraum (monatlich oder jährlich) untersucht wird. Der Servicekundenbericht enthält auch ein Diagramm zur täglichen Bandbreitennutzung, das einen detaillierteren Einblick in die tägliche Nutzung gewährt.

Vorgehensweise bei unzureichender Auslastung von Ressourcen

Nachdem Sie die unausgelasteten Ressourcen identifiziert und belegt haben, sollten Sie folgende Maßnahmen ergreifen, um die Probleme in der Auslastung zu beseitigen:

- Entfernen Sie ungenutzte Leitungen. Für den Fall, dass eine Mietleitung überhaupt nicht genutzt wird und auch nicht als Sicherung dient, können Sie die Leitung entfernen und so die monatlichen Kosten der Leitung einsparen.
- Stufen Sie die Kapazität von unausgelasteten Leitungen herab. Sie können häufig Kosten einsparen, indem Sie die Kapazität der Leitungen herabstufen. Diese Lösung ist besonders bei partiellem T1, Frame Relay-Schaltungen und ATM-Kanälen wirkungsvoll, kann sich jedoch als unpraktisch erweisen, wenn Sie auf andere Technologien umsteigen oder Kabel neu verlegen müssen.

- Leiten Sie den Verkehr auf eine unausgelastete Leitung um. Wenn Sie an ein und demselben Standort Leitungen mit zu hoher Auslastung verwenden oder Leitungen einsetzen, die zusammengelegt werden können, sollten Sie den Netzwerkverkehr ggf. auf eine unausgelastete Leitung umleiten. Wenn an dem betreffenden Standort kein weiterer Verkehr auftritt, sollten Sie folgende Möglichkeiten in Betracht ziehen:
 - > Verlagern Sie die lokalen Server an einen zentralen Standort, um den Verkehr auf der unausgelasteten Leitung zu erhöhen und durch die Zusammenlegung von Servern Kosten zu senken.
 - > Bündeln Sie den Datenverkehr verschiedener kleiner Lokalverbindungen an einem regionalen Knotenpunkt, der über eine gemeinsame Hochgeschwindigkeitsverbindung mit dem zentralen Standort kommuniziert.

Anzeigen des ROI

Nach Ermittlung der erforderlichen Kapazitätsänderungen können Sie die monatlichen Einsparungen berechnen, die sich infolge der entfernten Leitungen ergeben, und die Kostendifferenz zwischen den vorhandenen und den neuen herabgestuften Leitungen aufzeigen.

So schätzen Sie den ROI:

1. Prüfen Sie die monatlichen Nutzungsgebühren, um die Kosten der Mietleitungen zu ermitteln, die möglicherweise unausgelastet sind.
2. Setzen Sie sich mit Ihrem Serviceprovider in Verbindung, um die Kosten für die Änderung des Services sowie die monatlichen Kosten für die Änderung der Geschwindigkeit oder Bandbreite zu erfragen. Wenn bei der Änderung eines Services intern Kosten anfallen, beziehen Sie diese ebenfalls in die Berechnung ein.
3. Berechnen Sie den ROI für Serviceänderungen mit der folgenden Gleichung:

$$\text{ROI} = \text{Kosten für den Wechsel} / \text{monatliche Einsparungen}$$

In der folgenden Tabelle werden am Beispiel von drei Interfaces die anfallenden Kosten und Servicegebühren aufgeführt:

	NetLink	Chicago T1	Paxton T1
Aktuelle Geschwindigkeit	100 Mps	1,54 Mbps	1,54 Mbps
Neue Geschwindigkeit	10 Mbs	512 Kbs	128 Kbs
Aktuelle Kosten	\$3.300	\$2.500	\$5.000
Neue Kosten	\$2.500	\$2.000	\$3.200
Kosten für den Wechsel	\$5.000	\$1.000	\$1.200
Monatliche Einsparungen	\$800	\$500	\$1.800

4. Ermitteln Sie anhand der ROI-Berechnungen, ob die vorgeschlagenen Änderungen sinnvoll sind. In der Tabelle wird z. B. gezeigt, dass Sie durch die Herabstufung der NetLink-Leitung von 100 Mbs auf 10 Mbs monatlich \$800 einsparen können. Allerdings sind die bei diesem Wechsel anfallenden Kosten so hoch, dass sie sich erst nach sechs Monaten bezahlt machen. Wenn Sie stattdessen die Paxton T1-Leitung auf 128 Kbs herabstufen, zahlen sich die Investitionen bereits in weniger als einem Monat aus.

Aktualisierung der Konfiguration

Nachdem Sie Ihre Konfiguration so modifiziert haben, dass alle Kapazitätsprobleme gelöst sind, müssen Sie die SPECTRUM- und eHealth-Umgebungen aktualisieren, um diese an die neuen Geschwindigkeiten und ggf. an die ausgesonderten Ressourcen anzupassen.

So aktualisieren Sie die Konfiguration:

1. Aktualisieren Sie die SPECTRUM-Ansichten mit Hilfe der Rediscovery, um sicherzustellen, dass die Ansichten den aktuellen Stand der Geräte widerspiegeln.
2. Aktualisieren Sie die Polling-Konfiguration und Elementlisten von eHealth, indem Sie die Elementinformationen neu aus SPECTRUM importieren und eine Rediscovery der verwendeten Elemente durchführen. Wenn Sie künftig einen Bericht für die Zeitbereiche ausführen, in denen die Geschwindigkeit eines Elements geändert wurde, werden ggf. ungewöhnliche Auslastungsquoten (in Prozent) angezeigt.
3. Wenn Sie den Kapazitätsbedarf der vorhandenen Ressourcen verringern oder erhöhen, müssen Sie anschließend die Trend- und Health-Berichte für diese Ressourcen ausführen. Achten Sie auf mögliche Health-Ausnahmen oder andere Nutzungsprobleme, die infolge des erhöhten Verkehrs auftreten können.
4. Wenn Sie ein Element aussondern, müssen Sie das Polling deaktivieren und das Element aus der eHealth-Datenbank entfernen. Wenn Sie ein Element entfernen, können Sie für dieses Element so lange weiter Berichte erstellen, bis die zugehörigen Daten in der Datenbank veraltet sind.

Identifizierung der überlasteten Ressourcen

Führen Sie folgende Schritte aus, um die überlasteten Ressourcen zu identifizieren:

1. Suchen Sie nach den überlasteten Ressourcen.
2. Prüfen Sie, ob eine Überlastung vorliegt.
3. Entwickeln Sie eine Lösung für die überlasteten Ressourcen.

Suche nach überlasteten Ressourcen

Mit Hilfe der Kapazitätsplanungs-Tools von eHealth können Sie überlastete Ressourcen rechtzeitig identifizieren, bevor sie anfangen, Probleme zu bereiten. Wenn Sie einmal pro Woche einen Health-Bericht ausführen, können Sie die Netzwerkelemente ermitteln, deren Kapazität erreicht ist. Anschließend können Sie weitere Berichte ausführen, um die Probleme genauer zu analysieren und zu beseitigen, bevor das IT-Team drastischere Maßnahmen ergreifen muss.

So suchen Sie nach überlasteten Ressourcen:

1. Starten Sie die eHealth-Weboberfläche, und führen Sie einen täglichen Health-Bericht für den Wochentag mit der größten Auslastung aus.
2. Klicken Sie im linken Bereich des Health-Berichtsfensters auf „Exceptions Summary“, um den Ausnahmenzusammenfassungsbericht zu öffnen. Im Ausnahmenzusammenfassungsbericht werden die Elemente ermittelt, für die ungewöhnliche Vorfälle beobachtet wurden oder deren Ressourcen längere Zeit nicht in der Lage sind, den angeforderten Bedarf zu decken. Die Elemente sind nach dem Schweregrad der Ausnahme angeordnet, d. h., Elemente mit schwerwiegenden Problemen werden zuerst aufgeführt.

Exception Summary Report						
			Element	Ranking	Total	
Rank	Element Name	Speed	Type	Points	Exceptions	Leading Exception
1	Virginia	512 Kbs	Frame Relay	171.1	2	Utilization Health Index
2	Dallas-Houston	128 Kbs	Frame Relay	96.6	2	Utilization Health Index
3	Colorado	56 Kbs	Frame Relay	85.2	2	Congestion Health Index

3. Suchen Sie in dem Bericht nach den Elementen, für die in der Spalte „Leading Exception“ die Werte „Utilization Health Index“ oder „Congestion Health Index“ angezeigt werden. Diese Elemente müssen hohe Datenmengen bewältigen und sind ggf. überlastet.

In dem Beispiel wird an erster Stelle die Frame Relay-Verbindung zum Büro in Virginia angezeigt, die als Hauptausnahme einen „Utilization Health Index“ aufweist. Diese Verbindung ist mit großer Wahrscheinlichkeit überlastet und sollte weiter untersucht werden.

Bestätigung der überlasteten Ressourcen

Im Diagramm für zu beobachtende Situationen werden die Elemente angezeigt, die ihre Trendschwellenwerte laut Vorhersage fast bzw. ganz erreichen oder sogar überschreiten. Das Diagramm gibt an, wie stark sich die einzelnen Elemente ihren Schwellenwerten annähern, wie schnell die Auslastung wächst und wie lange es dauert, bis der Bedarf die vorhandene Kapazität übersteigt.

So überprüfen Sie, ob Ressourcen überlastet sind:

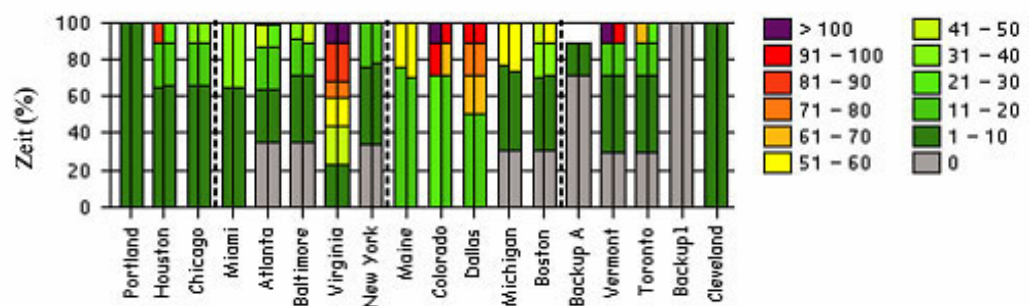
1. Führen Sie auf der eHealth-Weboberfläche einen Health-Bericht für die vergangene Woche aus.
2. Prüfen Sie das Diagramm für zu beobachtende Situationen im Abschnitt „Summary“ des Health-Berichts.

Zu beobachtende Situationen

Rang	Elementname	Variable	Schwellenwert Wert	Täglicher Durchschnitt		Tage bis (von) Schwellenwert
				Ist	Vorhergesagt	
1	Virginia (In)	Volume (Bandwidth %)	100.00	114.9	113.3	(2)
2	Dallas (Out)	Congestion (ppm Frames)	1000.00	908.5	908.2	1
3	Colorado (In)	Volume (Bandwidth %)	100.00	88.5	88.2	7
4	Maine (Out)	Volume (Bandwidth %)	100.00	8.5	3.3	Increasing
5	Michigan (Out)	Congestion (ppm Frames)	1000.00	188.5	114.2	Increasing

3. Überprüfen Sie die im Diagramm enthaltenen Elemente, und suchen Sie nach den Elementen, deren Schwellenwerte bereits überschritten sind oder deren Auslastung so stark zunimmt, dass die Schwellenwerte in Kürze erreicht sind. Während das erste Element (Virginia) in dem Beispiel seinen Schwellenwert bereits seit zwei Tagen überschritten hat, erreichen die nächsten beiden Elemente ihre Schwellenwerte laut Vorhersage erst in der kommenden Woche. Alle diese Elemente sind mit großer Wahrscheinlichkeit überlastet. Obwohl der Bedarf der letzten beiden Elemente weiter wächst, nehmen beide Elemente weniger als 20 % der Kapazität in Anspruch und stellen somit kein Problem dar.
4. Wählen Sie im Health-Bericht „Element Detail“, und überprüfen Sie das Diagramm zur Bandbreitennutzung für die Elemente, die ihrer Meinung nach zu stark beansprucht werden.

Bandbreitenauslastung

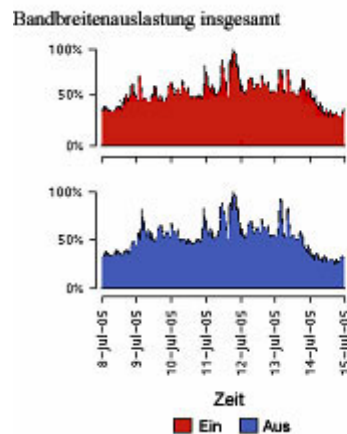


Das Diagramm zur Bandbreitennutzung gibt an, wie lange (in Prozent) sich die Elemente in den verschiedenen Stadien der Auslastung befinden. Die Farben Lila und Rot deuten i. d. R. auf eine überlastete Ressource hin. Lila deutet auf eine Auslastung von über 100 % hin. Vermutlich handelt es sich um eine Mietleitung, die die vertraglich vereinbarte Bandbreite überschreitet, wobei für die überschüssige Bandbreite zusätzliche Gebühren fällig werden.

5. Untersuchen Sie das Diagramm, um zu ermitteln, wie oft das verdächtige Element während der letzten Woche überlastet wurde. Bei bestimmten Elementen besteht zwar permanent ein hoher Bedarf (z. B. bei der Virginia-Leitung), da der Bedarf über einen längeren Zeitraum jedoch schwankt, weisen die meisten Elemente beträchtliche Phasen mit geringerer Auslastung auf. Je nach Netzwerkaktivität kann es vorkommen, dass ein Element zu bestimmten Zeiten überhaupt nicht genutzt wird (z. B. über Nacht), aber dennoch überlastet ist, weil der Bedarf die Kapazität zu den Spitzenzeiten übersteigt.

Die Vermont-Leitung wird z. B. ein Drittel der Zeit (möglicherweise über Nacht) überhaupt nicht genutzt und weist die meiste Zeit eine Auslastung von weniger als 20 % auf. Da die Auslastung von 100 % zu den Spitzenzeiten jedoch überschritten wird, könnten zusätzliche Kosten entstehen, weshalb die Leitung als überlastet gilt.

6. Wenn Sie weitere Details zur Performance eines Elements benötigen, erstellen Sie einen Übersichtsbericht, indem Sie im Diagramm zur Bandbreitennutzung auf das betreffende Element klicken.



7. Prüfen Sie die Diagramme zur Bandbreitennutzung im Übersichtsbericht, um zu ermitteln, wie häufig und in welchen Zeiträumen das betreffende Element überlastet wurde. Das Beispieldiagramm gibt an, dass das Element zwar den größten Teil der Woche nur zu 50 % ausgelastet war, dafür aber mehrmals den Schwellenwert von 100 % erreicht hat. Es hängt von den jeweiligen Geschäftsanforderungen ab, ob ein Element, dass lediglich einmal pro Woche seine volle Kapazität erreicht, noch tragbar ist, oder ob eine etwa einstündige Überlastung bereits ein ernstzunehmendes Problem darstellt, insbesondere wenn die Überlastung zu den Hauptgeschäftszeiten auftritt.

8. Überprüfen Sie die anderen Diagramme im Übersichtsbericht auf mögliche Abweichungen, z. B. hohe Fehlerraten oder Anzeichen für Blockierungen (FECNs – Forward Explicit Congestion Notifications, BECNs – Backward Explicit Congestion Notifications oder Löschungen). Ermitteln Sie anhand dieser Informationen, welche Bedingungen sich möglicherweise nachteilig auf das Element auswirken, wie z. B.:
 - > Unzureichende Kapazität
 - > Ineffiziente oder falsch konfigurierte Anwendungen, die eine zu hohe Bandbreite verbrauchen
 - > Anzahl der Stationen (zu viele oder zu wenige), die zu einer Überlastung der WAN-Verbindung führen kann
 - > Eine häufig wiederholte oder überbrückte Domäne, die weitergeleitet werden sollte
9. Erstellen Sie einen Berichtsverlauf für die überlasteten Ressourcen, der die hohe Auslastung belegt. Neben den bereits beschriebenen Berichten können Sie im Ausnahmenzusammenfassungsbericht und im Diagramm für zu beobachtende Situationen Detailberichte zu den betreffenden Elementen ausführen. Außerdem können Sie für bestimmte Elemente den Bandbreitentrend-Bericht ausführen, um die langfristige Auslastung der Ressourcen zu analysieren.

Vorgehensweise bei Überlastung von Ressourcen

Wenn Sie die überlasteten Ressourcen identifiziert und dokumentiert haben, sollten Sie entsprechende Maßnahmen zur Beseitigung der Probleme ergreifen:

- Richten Sie für das betreffende Element eine größere Kapazität ein.
- Leiten Sie den Bedarf auf andere Ressourcen um.
- Fügen Sie zusätzliche Elemente hinzu, um die Arbeitslast zwischen mehreren Ressourcen aufzuteilen.

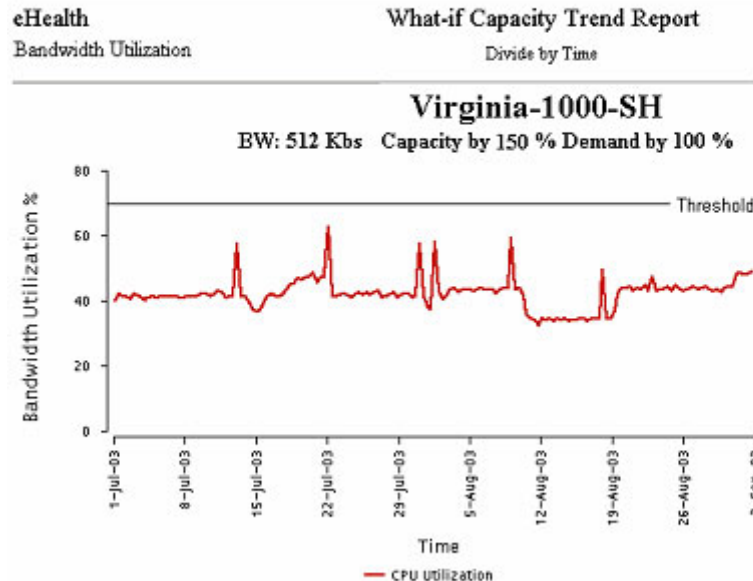
BEST PRACTICE

Visualisieren Sie mit Hilfe der konditionalen Kapazitätstrendberichte, wie sich die höhere Kapazität oder der verringerte Bedarf auf das überlastete Element auswirken, und ermitteln Sie die optimale Kapazität aller neuen Ressourcen. Wenn Sie den Bericht ausführen, müssen Sie ein Element, eine Kapazitätsvariable und einen Zeitbereich angeben. Der Bericht gibt den Wert dieser Performancevariable während des ausgewählten historischen Bereichs an.

Der konditionale Bericht weist große Ähnlichkeit mit dem eHealth-Trendbericht auf. Allerdings können Sie hier auch die Kapazität der Ressource ändern oder den Bedarf anpassen, der während dieses Zeitraums von der Ressource gefordert wird, oder beides. Anschließend können Sie den Bericht aktualisieren, um die Auswirkungen der möglichen Änderungen zu modellieren.

Hinweis: Beachten Sie, dass die Werte für Kapazität und Bedarf als Prozentwerte angegeben werden müssen. Die Eingabe von 100 % führt z. B. dazu, dass die aktuellen Werte verwendet werden. Bei Eingabe von 50 % werden die aktuellen Werte halbiert (Kapazität oder Bedarf werden durch 2 geteilt), und bei Eingabe von 200 % werden die aktuellen Werte verdoppelt.

What-if Capacity Trend Report
 Virginia-1000-SH Bandwidth Utilization
 Adjust actual capacity by and demand by



Der Bericht gibt an, dass, wenn die Kapazität der Virginia-Leitung um 50 % erhöht wird (Kapazität = 125 %), sich die Spitzenauslastung auf 60 % der Kapazität verringert. Diese Kapazität sollte ausreichen, um den erwarteten Bedarf zu decken.

Planung zukünftiger Kapazitätsänderungen

Führen Sie folgende Schritte aus, um Kapazitätsänderungen zu planen und vorherzusagen:

1. Identifizieren Sie die potenziellen Kapazitätsänderungen.
2. Analysieren Sie die Kapazitätstrends.
3. Visualisieren Sie die Kapazitätsänderungen.
4. Nehmen Sie die gewünschten Kapazitätsänderungen vor.

Identifizierung potenzieller Kapazitätsänderungen

eHealth stellt Berichte zur Kapazitätsplanung bereit, mit deren Hilfe Sie das Verhalten der Ressourcen unter wechselnden Bedingungen analysieren und vorhersagen können, wann und wo weitere Kapazitäten benötigt werden.

So identifizieren Sie potenzielle Kapazitätsprobleme:

1. Planen Sie einen Health-Bericht ein, der immer sonntags ausgeführt wird, um die Daten der gesamten Geschäftswoche auszuwerten. Eine entsprechende Anleitung finden Sie im Abschnitt zur Anpassung und Einplanung von Health-Berichten in Kapitel 5 dieses Handbuchs.
2. Analysieren Sie das Diagramm für zu beobachtende Situationen im Abschnitt „Summary“ des Health-Berichts. Im Diagramm für zu beobachtende Situationen werden die Top-10-Elemente (Netzwerkinterfaces, CPUs, Festplattenpartitionen) angezeigt, die sich der Grenze ihrer Kapazität annähern. Das Diagramm gibt an, wie stark sich die einzelnen Elemente ihren Schwellenwerten annähern, wie schnell die Auslastung wächst und wie lange es dauert, bis der Bedarf die vorhandene Kapazität übersteigt.

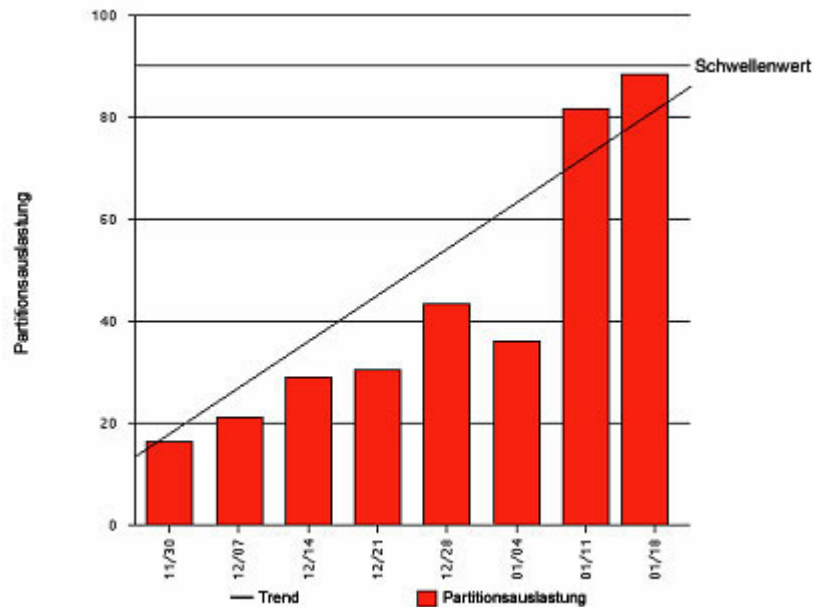
Zu beobachtende Situationen

Rang	Elementname	Variable	Schwellenwert	Wöchentlicher Durchschnitt		Tage bis (von)
			Wert	Ist	Vorhergesagt	Schwellenwert
1	System-Orange	Partition Utilization	90.000	88.663	90.191	0
2	System-Green	Partition Utilization	90.000	82.012	81.942	20
3	System-Purple	Partition Utilization	90.000	41.202	46.580	80
4	System-Black	Virtual Memory Utilization	90.000	40.000	43.469	86
5	System-White	Partition Utilization	90.000	70.620	71.686	144
6	System-Pink	Partition Utilization	90.000	45.746	47.685	Increasing
7	System-Brown	Partition Utilization	90.000	41.620	40.042	Decreasing

In dem Bericht werden mehrere Benutzerpartitionen angezeigt, die sich dem Schwellenwert annähern. Für das System-Orange wird in der Spalte „Days To Threshold“ der Wert „0“ angezeigt, was darauf hindeutet, dass der Trendschwellenwert bereits erreicht ist. Das System-Green wird seinen Schwellenwert dagegen erst in 20 Tagen erreichen, und für das System-Pink wird der Wert „Zunehmend“ angezeigt, was darauf hindeutet, dass die Auslastung zwar weiter wächst, der Schwellenwert jedoch erst in geraumer Zeit erreicht sein wird.

Alle Systeme, die sich an oder nahe ihrem Schwellenwert bewegen, sollten genauer untersucht werden. Es könnte z. B. sein, dass das System-Orange bereits überlastet ist. Es könnte sich jedoch auch um eine Systempartition handeln, die darauf ausgelegt ist, mit voller Kapazität zu arbeiten. Das System-Green, das seinen Schwellenwert erst in 20 Tagen erreichen wird, ist dagegen ein guter Kandidat für eine Aktualisierung, insbesondere wenn der Bedarf an dem System weiter steigt.

3. Wenn Sie weitere Informationen zu den beobachteten Situationen anzeigen möchten, klicken Sie auf den Namen des Elements, um für die betreffende Partition den Detailbericht für zu beobachtende Situationen auszuführen.



4. Analysieren Sie die Trendlinie, um zu ermitteln, wie schnell sich die Auslastung dem Schwellenwert annähert. Wenn die Linie, wie im Beispiel, kontinuierlich ansteigt, sollten Sie die Kapazität anpassen, indem Sie die Größe der Partition erhöhen, unbenötigte Verzeichnisse oder Dateien löschen oder ein neues System erwerben.

Analyse von Kapazitätstrends

Wenn Sie die potenziellen Kandidaten für die Aktualisierung identifiziert haben, führen Sie den Kapazitätsprojektionsbericht und den Kapazitätsbereitstellungsbericht aus, um die Volumenänderungen für die nächsten Wochen und Monate vor auszuplanen und vorherzusagen, wann Elemente aktualisiert werden müssen.

So führen Sie den Kapazitätsprojektionsbericht und den Kapazitätsbereitstellungsbericht aus:

1. Melden Sie sich auf der eHealth-Web Oberfläche an, und klicken Sie auf die Registerkarte „Run Reports“.
2. Klicken Sie auf die Verknüpfung für den Health-Standardbericht. Daraufhin wird die Seite „Run Health Report“ angezeigt.
3. Geben Sie die Berichtsmerkmale an (z. B. Systemtechnik und eine Gruppe von Elementen).

4. Klicken Sie auf „More Options“, und führen Sie folgende Schritte aus:
 - a. Wählen Sie unter „Presentation Attributes“ den Eintrag „Capacity“ aus.
 - b. Wählen Sie für die Berichte „Capacity Projection“ und „Capacity Provisioning“ aus.
 - c. Geben Sie im Feld „Capacity Provisioning Minimum Lead-Time“ den Wert „20“ ein.
 - d. Geben Sie im Feld „Capacity Provisioning Maximum Lead-Time“ den Wert „90“ ein.
5. Geben Sie einen eindeutigen Namen, z. B. „Capacity_Report“, für den Bericht ein, und speichern Sie ihn als Vorlage.
6. Klicken Sie auf „Generate Report“, um den Bericht auszuführen. Wenn der Bericht auf Anforderung ausgeführt wird, kann der Vorgang einige Minuten in Anspruch nehmen. Als Best Practice empfiehlt es sich, den Bericht von der eHealth-Konsole auszuführen. Auf diese Weise wird der Bericht automatisch außerhalb der Spitzenzeiten erstellt und steht bei Bedarf zur Prüfung bereit.
7. Prüfen Sie den Kapazitätsprojektionsbericht. Der Bericht sagt vorher, wie sich die Kapazität einer bestimmten Variablen (z. B. die Auslastung einer Partition) in nächster Zukunft verändert. Sie können den Bericht auf Basis von Spitzen-, Durchschnitts- oder prozentualen Kapazitätswerten ausführen. eHealth wägt die prognostizierten Kapazitätswerte gegen den angegebenen Schwellenwert ab und zeigt die Elemente an, die den Schwellenwert laut Vorhersage überschreiten werden.

Partitionskapazitätsprojektion

	Schwellenwert	Wöchentlicher Durchschnitt			
Elementname	Wert	Ist	30 Tage	90 Tage	9 Monate
System-Orange	90.000	88.663	88.686	90.063	90.580
System-Green	90.000	82.012	90.042	90.932	90.520
System-Purple	90.000	41.202	41.202	90.000	90.101
System-White	90.000	70.620	70.620	71.686	90.167
System-Pink	90.000	45.746	45.963	55.746	60.000
System-Brown	90.000	41.620	41.020	40.000	40.000

Der Bericht gibt an, welcher Prozentsatz der Partitionskapazität von den einzelnen Systemen in den nächsten 30 Tagen, 90 Tagen und neun Monaten verbraucht wird. Wie Sie sehen, hat der Bedarf von System-Orange den Schwellenwert fast erreicht, steigt jedoch kaum weiter an. Der Bedarf von System-Purple nimmt dagegen stetig zu und wird schon bald seine Kapazität erreichen. Das System-Purple sollte daher dringend aktualisiert werden.

8. Prüfen Sie den Kapazitätsbereitstellungsbericht, um zu ermitteln, wann die Elemente laut Vorhersage aktualisiert werden müssen. Der Kapazitätsbereitstellungsbericht vergleicht die prognostizierten Kapazitätswerte mit einem Aktualisierungsschwellenwert und zeigt die Elemente an, die den Schwellenwert laut Vorhersage überschreiten. Der Bericht gibt auch an, in wie viel Tagen eine Aktualisierung erforderlich ist.

Kapazitätsbereitstellung 20-90 Tage Vorlaufzeit, 90% Aktualisierungszeitpunkt

		Täglicher Durchschnitt	Tage bis
Elementname	Variable	Ist	Aktualisierung
System-Green	Partition Utilization	82.012	20.00
System-Purple	Partition Utilization	41.202	80.00
System-Black	Virtual Memory Utilization	40.000	86.00

Sie können den Bericht, ähnlich wie den Kapazitätsprojektionsbericht, auf Basis von Spitzen-, Durchschnitts- oder prozentualen Kapazitätswerten ausführen. Sie können sowohl den Schwellenwert als auch die Vorlaufzeit der Aktualisierung festlegen, indem Sie die Präsentationsattribute des Health-Berichts anpassen.

In dem Bericht werden die Elemente angezeigt, die innerhalb der nächsten 20 bis 90 Tage für 90 % ihrer Kapazität einen Aktualisierungszeitpunkt erreichen. System-Green benötigt am dringendsten ein Upgrade, das in den nächsten 20 Tagen durchgeführt werden sollte.

BEST PRACTICES

Für die Kapazitätsprojektions- und Bereitstellungsberichte ist es wichtig zu wissen, wie viel Vorlaufzeit benötigt wird, um neue Kapazitäten online zu bringen. Einige Serviceanbieter benötigen z. B. 90 Tage, um eine neue T1-Leitung bereitzustellen. Bei Systemen dauert es möglicherweise 30 Tage, um neuen Festplatten- oder Arbeitsspeicher zu bestellen und hinzuzufügen. Sie müssen also wissen, wann Sie für die verwalteten Ressourcen weiteren Speicher bestellen müssen, damit dieser verfügbar ist, d. h. installiert, getestet und implementiert, bevor der Aktualisierungszeitpunkt erreicht ist.

In diesen Berichten werden die Standorte angegeben, für die heute zusätzliche Kapazitäten bestellt werden müssen, damit der kritische Punkt nicht erreicht wird. Bei den Beispielen in diesem Abschnitt wird eine Vorlaufzeit von 20-90 Tagen angenommen, an allen drei Standorten ist eine Aktualisierung in diesem Zeitfenster erforderlich. Wenn das Hinzufügen von Speicherplatz länger als 90 Tage in Anspruch nimmt, wird der Aktualisierungsschwellenwert von 90 % höchstwahrscheinlich in diesem Zeitraum überschritten. Am Anfang werden Sie beim Einsatz von eHealth zur Überwachung Ihrer Ressourcen eventuell feststellen, dass für einige Ressourcen bereits vor Ablauf der Vorlaufzeit eine Aktualisierung erforderlich ist. Mit der Zeit werden Sie anhand dieser Berichte jedoch Probleme früher isolieren und diese Schwellenwertüberschreitungen vermeiden, bevor das Vorlaufzeitfenster abläuft.

Visualisierung von Kapazitätsänderungen

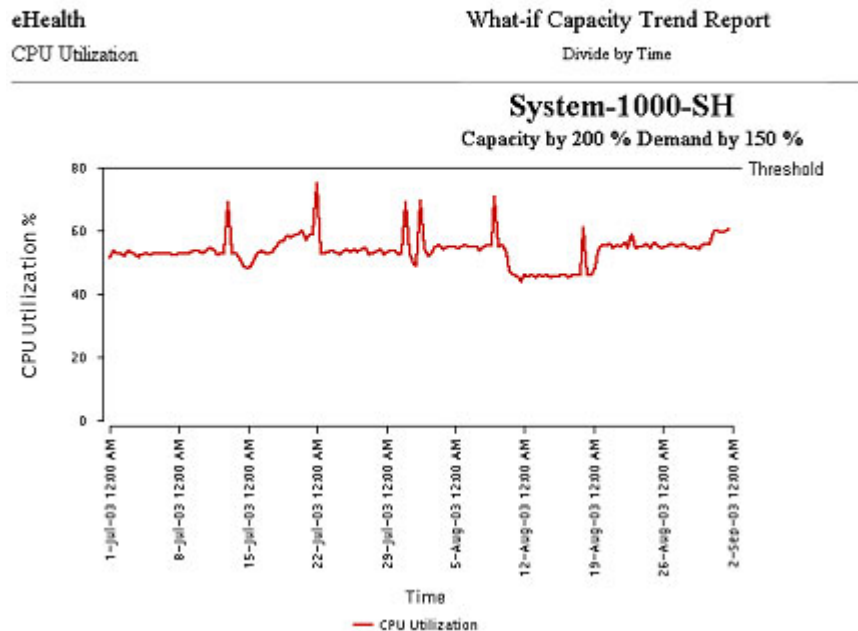
Der konditionale Kapazitätstrendbericht zeigt, wie sich Ressourcen bei Änderungen und Ausweitungen Ihrer Infrastruktur verhalten. Diese Berichte ermöglichen Ihnen, historische Daten zur Vorhersage zukünftiger Muster heranzuziehen, Änderungen der Kapazität und des Bedarfs zu modellieren und die Auswirkungen auf Ressourcen zu bestimmen.

So können Sie die Auswirkungen von Bedarfsänderungen visualisieren:

1. Führen Sie zur Analyse der potenziellen Lösungen einen konditionalen Kapazitätstrendbericht aus:
 - a. Wählen Sie auf der Seite „Run Reports“ in der Spalte „Available Reports“ unter „What-If“ die Option „CapacityTrend“ oder den Namen einer anderen Vorlage aus. Es wird die Seite „Run a Capacity Trend What-If Report“ geöffnet.
 - b. Wählen Sie in der Liste „Element Type“ einen Elementtyp und anschließend in der Liste der verfügbaren Elemente ein Element aus.
 - c. Wählen Sie eine Variable für Ihren Bericht aus.
 - d. Wählen Sie unter „Chart type“ ein Diagrammformat aus.
 - e. Geben Sie unter „Divide by“ an, wie die ausgewählte Variable grafisch dargestellt werden soll.
 - f. Wählen Sie gegebenenfalls ein Zeitintervall aus, in dem die Daten kumuliert werden.
 - g. Wählen Sie auf der Grundlage des Zeitbereichs für den Bericht eine Beispielgröße aus. Bei der Beispielgröße „As Is“ werden die detailliertesten verfügbaren Daten verwendet und die Werte werden nicht kumuliert.
 - h. Wählen Sie unter „Report Time“ den Berichtszeitraum aus. Sie können die Werte „now“, „today“, „yesterday“ oder einen Datumswert bzw. Zeitwert angeben.
 - i. Wählen Sie „More Options“ aus, um die Stunden und Tage anzugeben, die der Bericht anzeigen soll.
 - j. Sie können den Bericht gegebenenfalls anpassen, indem Sie die Präsentationsattribute festlegen.
 - k. Klicken Sie auf „Generate Report“.

- Passen Sie in den Feldern oben auf dem Bericht die Kapazität und/oder den Bedarf für die Ressource an, und generieren Sie zur Modellierung der Änderung den Bericht erneut.

What-if Capacity Trend Report
 System-1000-SH CPU Utilization
 Adjust actual capacity by and demand by



- Modellieren und bestimmen Sie anhand des Berichts, ob eine vorhandene Ressource die erwarteten Änderungen unterstützen kann, und wenn nicht, wie viel zusätzliche Kapazität benötigt wird. Darüber hinaus können Sie potenzielle Probleme darstellen, so dass Sie Anforderungen für neue Ausrüstungsteile oder Aktualisierungen vorschlagen können.

Dieser Bericht zeigt beispielsweise, dass durch Verdoppelung der CPU-Kapazität der Bedarf auf dem Server auch bei einem Bedarfsanstieg von 50 % weit unter dem Trendschwellenwert von 80 % liegen wird.

Vorgehensweise bei Kapazitätsänderungen

Nachdem Sie mögliche Kapazitätsprobleme oder -verbesserungen erkannt haben, erwägen Sie eine dieser typischen Aktionen zur Lösung des Problems:

- Aktualisieren des Elements auf eine höhere Kapazität
- Ersetzen des Elements durch ein größeres oder schnelleres Gerät (z. B. eine größere Festplatte, ein schnelleres Interface oder ein schnelleres CPU-System)

Mit dem konditionalen Bericht können Sie modellieren bzw. visualisieren, wie die vorgeschlagenen Änderungen die Performance verbessern werden. Nachdem Sie Änderungen an Ihren Geräten oder Ressourcen vorgenommen haben, aktualisieren Sie die Konfiguration wie in Kapitel 5 beschrieben.

Planung von Sprachkapazitäten

Bei Netzwerken mit herkömmlichen bzw. IP-Sprachtelefoniegeräten oder Voice-Messaging-Systemen kann eHealth for Voice hilfreich sein, um Kapazitätsprobleme zu identifizieren und den GoS in den Spitzenbelastungsstunden des Netzwerks zu überwachen. Bei Sprachgeräten können Kapazitätsprobleme durch die Verbindungs-/Portnutzung und den Speicherplatz für Sprachnachrichten verursacht werden. Wenn diese Faktoren überbeansprucht werden, führt das zu Serviceverschlechterungen und beeinträchtigt die Kundenzufriedenheit. Werden diese Faktoren unterbeansprucht, ist es wichtig zu bestimmen, wo Ihre Geräte überversorgt sind, so dass Sie Schritte zur Kostenreduzierung oder Neuordnung von Ressourcen einleiten können, um Überlastungen in anderen Bereichen des Netzwerks auszugleichen.

Durch eine effektive Kapazitätsplanung können Sie Folgendes erreichen:

- Verringern von Kosten durch Reduzierung oder Eliminierung von unterbeanspruchten Mietleitungen sowie Reduzierung der Wartungskosten für nicht verwendete oder unnötige Ports.
- Verbessern der Performance durch Bestimmung der über- und unterbeanspruchten Ports bzw. Verbindungen und Anpassen der Kapazität an den Bedarf.
- Verbessern der Budgetvorhersagbarkeit durch Nachverfolgen von Trends, wodurch Sie Notkäufe vermeiden und sicherstellen können, dass Sie zu den günstigsten Servicekosten planen können.

Um Verkehrsmuster zu verstehen, müssen Sie Informationen aus der PBX sammeln, die Details zu den Verkehrsspitzen für die einzelnen Verbindungsgruppen für mindestens einige Wochen, vorzugsweise sogar Monate liefern. Diese Informationen sind über den Switch verfügbar. eHealth for Voice automatisiert die Sammlung dieser Informationen, wodurch es leichter wird, quartalsweise und nach Bedarf Wartungsbewertungen der Sprachkapazität und der Verwendungsmuster auszuführen.

Analyse von Sprachkapazitäten

Wenn Sie Informationen zum Verkehr für den gewünschten Zeitraum gesammelt haben, können Sie mit dem Capacity Analyzer bestimmen, wie gut die Sprachgeräte ihre Funktion während der Verkehrsspitzenzeiten erfüllen. In diesem Dialogfeld können Sie auf schnelle Weise den GoS kalkulieren sowie Speicherkapazitäten der Nachrichtenserver und die Prozesskapazität der Kommunikationsserver anzeigen.

So greifen Sie auf Capacity Analyzer zu:

1. Wählen Sie im Startmenü des Systems, in dem eHealth for Voice installiert ist, „Programme“, „eHealth for Voice“ und dann „eHealth for Voice“. Die Programmkonsole von eHealth for Voice wird angezeigt.
2. Wählen Sie in der linken Navigationskonsolenstruktur „Measurements“ und „Reports“.

3. Doppelklicken Sie im rechten Konsolenbereich auf das Symbol für Capacity Analyzer. Das Dialogfeld „Capacity Analyzer“ wird angezeigt.

Node Name/Id	Trunk Group Name	Trunk Group No.	Busy Day	Busy Hour	Erlangs	Actual GOS	Trunks Equipped
Definity G3 LA / 4	Amcon PRI-1	1	4/23/2006	00:00	20.5	0.1	23
Definity G3 LA / 4	Amcon PRI-2	2	4/23/2006	00:00	20.5	0.1	23
Definity G3 LA / 4	Amcon PRI-3	3	4/23/2006	00:00	0	0.001	23
Definity G3 LA / 4	Amcon PRI-4	4	4/23/2006	00:00	0	0.001	23
Definity G3 LA / 4	to HQ, TG74	10	4/23/2006	00:00	0	0.001	23
Definity G3 LA / 4	to EIVR DS1	11	4/23/2006	00:00	0	0	0
Definity G3 LA / 4	H 323 ICC	12	4/23/2006	00:00	0	0.001	3
Definity G3 LA / 4	OUTSIDE CALL	20	4/23/2006	00:00	0	0.001	23
Definity G3 LA / 4	H 323 PBX7, TG30	30	4/23/2006	00:00	0	0.001	3
Definity G3 LA / 4	f1 PRI to Mlink 78	36	4/23/2006	00:00	0	0	0
Definity G3 LA / 4	H 323 to Mlink 147	38	4/23/2006	00:00	0	0.001	10

Analyse von GoS

eHealth for Voice berechnet einen GoS, um zu bestimmen, wie die Betreuung für Anrufer (beantwortete Anrufe, besetzt oder unbeantwortete Anrufe) während der geschäftigsten Stunde des Zeitraums ist. Dadurch können Sie bestimmen, wie viel zusätzliche Bandbreite für den Sprachverkehr im Netzwerk benötigt wird.

So analysieren Sie den GoS:

1. Öffnen Sie im Dialogfeld „Capacity Analyzer“ die Registerkarte „Port Analysis“, um auf das Berechnungstool für den Grade of Service zuzugreifen. Der Ziel-Grade-of-Service bezieht sich auf den prozentualen Anteil von Anrufern, der während der geschäftigsten Stunde betreut wird (beantwortete Anrufe). Ein GoS von 0,001 besteht, wenn 0,999 % der Anrufer durchkommen.
2. Wählen Sie den Ziel-GoS aus, und klicken Sie auf „Apply“. Im Dialogfeld wird die Anzahl der Verbindungen angezeigt, die zur Erfüllung dieses Ziel-GoS zusätzlich benötigt werden.

3. Blättern Sie mit der horizontalen Scrollleiste zur rechten Seite des Dialogfelds.

Capacity Analyzer

Platform: ☒ Definity/Comm Man
☐ Intuity
☐ Modular Messaging
☐ Nortel

Node: ☒ ALL
☐ Definity G3 LA:4
☐ Definity NY:5
☐ Lab G3:20

Start Date: 03/25/2005
End Date: 04/25/2006

Date Breakdown: None
Source: Trunk Group

Port Analysis | Disk Analysis | Processor

Target GOS: .001
Trunk Group No.: ALL

	Erlangs	Actual GOS	Trunks Equipped	Trunks Required	Add/(Delete) Trunks	Total Attempts	Trunk Gp Dir
▶	20.5	0.1	23	35	12	5702	two
	20.5	0.1	23	35	12	5698	two
	0	0.001	23	2	(21)	0	two
	0	0.001	23	2	(21)	0	two
	0	0.001	23	2	(21)	0	two
	0	0	0	2	2	0	two
	0	0.001	3	2	(1)	0	two
	0	0.001	23	2	(21)	0	two
	0	0.001	3	2	(1)	0	two
	0	0	0	2	2	0	two
	0	0.001	10	2	(8)	0	two
	13.69	0.007	23	26	3	96	out
	6.72	0.001	23	17	(6)	143	inc

Buttons: Apply, Clear, Cancel, Print Grid, Export Grid

4. Entnehmen Sie der Spalte „Add/(Delete) Trunks“ die Anzahl der Verbindungen, die Sie zur Erfüllung dieses GoS benötigen. Die Zahl in Klammern gibt die Anzahl der Verbindungen an, die entfernt werden können, ohne den gewünschten GoS in der Spitzenstunde gefährden zu müssen. So können Sie unterbeanspruchte Ressourcen leicht identifizieren.
5. Der Spalte „Erlangs“ können Sie den Ist-Spitzenverkehr entnehmen. Ein Erlang ist ein Maß für die Kapazität des Sprachverkehrs. Es gibt an, wie viele Minuten Sprachverkehr während einer Zeitstunde stattfindet. Wenn 10 Benutzer jeweils einen 10-minütigen Anruf in einer bestimmten Stunde tätigen, enthält diese Stunde 100 Anrufminuten und somit 1,67 Erlangs Sprachverkehr. Diese Informationen sind hilfreich zur Bestimmung der zusätzlich erforderlichen Bandbreite, die für das Netzwerk zur Unterstützung des Sprachservices benötigt wird.

BEST PRACTICES

Berücksichtigen Sie beim Einsatz von Capacity Analyzer die folgenden Best Practices, durch die Sie zu aussagekräftigeren Ergebnissen für Ihre Umgebung kommen können:

- Führen Sie Capacity Analyzer zu Beginn des Einsatzes von eHealth for Voice wöchentlich aus, um Ressourcen zu identifizieren, die nicht verwendet werden. Nach dieser Anfangsphase können Sie das Programm weniger häufig (monatlich oder vierteljährlich) ausführen, um die Auslastungsänderungen des Netzwerks zu beobachten.
- Verbindungs- oder Port-Leitungen mit keinem oder sehr geringem Verkehr könnten als Sicherungs- oder Überlaufleitungen dienen. Halten Sie stets Rücksprache mit dem verantwortlichen Techniker für PBX/IP-PBX, bevor Sie detaillierte Änderungspläne für Services machen, um sicherzustellen, dass Ihnen die Aufgaben der jeweiligen Verbindungen oder Ports bekannt sind.
- Der Über- und Unterlastungsgrad variiert je nach ausgewähltem GoS. Mit sinkendem GoS steigt der Bedarf an zusätzlichen Ressourcen. Mit Hilfe von Unternehmens-Service-Levels lässt sich der für Ihre Umgebung benötigte GoS leichter definieren.

Vorgehensweise bei unzureichender Auslastung von Ressourcen

Nachdem Sie unterbeanspruchte Ressourcen identifiziert und dokumentiert haben, sollten Sie in Betracht ziehen, nicht beanspruchte Verbindungen, Ports oder PBXs zu eliminieren, um die Service- und/oder Wartungskosten für Ihr Netzwerk zu reduzieren.

Anzeigen des ROI

Nachdem Sie die möglichen Kapazitätsänderungen identifiziert haben, können Sie die potenziellen monatlichen Einsparungen durch eliminierte Verbindungen und die Differenz der Wartungskosten zwischen aktuellen und zukünftigen Konfigurationen berechnen und anzeigen.

So schätzen Sie den ROI:

1. Bestimmen Sie anhand der monatlichen Nutzungsgebühren die Kosten für die Mietleitungen, die eventuell unterbeansprucht sind.
2. Anhand der Port-Wartungsgebühren können Sie die Kosten für nicht verwendete Ports ermitteln.
3. Setzen Sie sich mit Ihren Serviceanbietern in Verbindung, um die anfallenden Kosten für Änderungen des Services oder eine Reduzierung der Anzahl von Ports zu erfahren. Wenn bei der Änderung eines Services intern Kosten anfallen, beziehen Sie diese ebenfalls in die Berechnung ein.
4. Berechnen Sie mit der folgenden Gleichung den ROI für Serviceänderungen:
$$\text{ROI} = (\text{Servicegebühren} + \text{Port-Änderungsgebühr}) / \text{monatliche Einsparungen}$$
5. Entscheiden Sie auf der Grundlage Ihrer ROI-Berechnungen, ob die vorgeschlagenen Änderungen sinnvoll sind.

Bestätigung und Vorgehensweise bei Überlastung von Ressourcen

Capacity Analyzer gibt den Spitzenverkehr für einen bestimmten Zeitrahmen sowie die zur Bewältigung des Verkehrsaufkommens für den gewünschten Grade of Service benötigte Anzahl an Verbindungen oder Ports an.

Um die Ergebnisse der Überbeanspruchung zu bestätigen, gehen Sie wie folgt vor:

- Führen Sie Capacity Analyzer erneut für einen kleineren Datumsbereich aus. Wenn beispielsweise in einem Quartalsbericht Spitzenstunden angegeben werden, in denen die Auslastung auffällig ist, werten Sie die einzelnen Monate aus, um das Muster bzw. den Trend der Spitzenstundendaten zu bestimmen. So können Sie feststellen, ob die Stunde mit starkem Verkehrsaufkommen eine Anomalie darstellt oder ob der Verkehr im Netzwerk generell zunimmt. Wenn die Stunde mit hohem Verkehrsaufkommen auf ein einmaliges Ereignis zurückzuführen ist, können Sie diese atypische Aktivität bei Ihrer Kapazitätsplanung ignorieren.
- Durch das Erstellen von Sprachverkehrsberichten für die Plattform lassen sich Trends bei der Verbindungs- oder Port-Auslastung ausmachen. Auf diese Weise können Sie feststellen, ob ein Überlauf in eine andere Verbindungsgruppe stattfindet.
- Bestätigen Sie den ausgewählten GoS beim verantwortlichen Techniker für PBX/IP-PBX für diese Verbindungsgruppe. Bestätigen Sie, dass bei der Analyse der einzelnen Verbindungsgruppen der GoS verwendet wird, der ursprünglich für diese Gruppe bestimmt oder geplant war.
- Wenden Sie sich an Ihren Serviceanbieter, um weitere Kapazitäten hinzuzufügen, z. B. durch Hinzufügen von Verbindungen zur Hunt-Gruppe oder durch Hinzufügen von mehr Kapazität zu einer partiellen T1-Leitung.

Analyse des Festplattenspeichers für Voice Messaging

Mit Capacity Analyzer haben Sie die Möglichkeit, die Kapazität des Nachrichtenbereichs für die Sprachnachrichtenservices zu prüfen. Wenn kein freier Speicherplatz verfügbar ist, können Benutzer keine Sprachnachrichten erstellen. Bei Unternehmen, die über Sprachnachrichten Aufträge entgegennehmen oder Ressourcen verwalten, können Speicherplatzprobleme kritische Serviceeinbußen verursachen.

So analysieren Sie den Festplattenspeicher für Sprachnachrichten:

1. Öffnen Sie im Dialogfeld „Capacity Analyzer“ die Registerkarte „Voice Messaging Disk Analysis“.
2. Im Dialogfeld finden Sie Information zur Speicherauslastung und Statistiken zu den betriebsreichen Tagen, mit denen Sie leichter bestimmen können, ob die Sprachnachrichtenserver das normale Volumen bewältigen können und welcher der betriebsreichste Tag war.

Lösung von Festplattenspeicherproblemen

Wenn Ihren Nachrichtenservices nicht mehr genügend Festplattenspeicher zur Verfügung steht, führen Sie die folgenden Schritte aus, um die Kapazitätsprobleme zu lösen:

- Fordern Sie die Benutzer auf, alte/nicht mehr benötigte Nachrichten zu löschen, um Speicherplatz freizugeben.
- Ziehen Sie in Erwägung, Beschränkungen für die Länge der Sprachnachrichten, die zeitliche Aufbewahrung von Nachrichten und die Anzahl der gespeicherten Nachrichten einzuführen. Dadurch wird der durch Mailboxes belegte Speicherplatz vorhersehbarer.
- Wenn durch die Einsparungsverfahren nicht ausreichend Speicherplatz freigegeben wird, teilen Sie den Messaging-Servern zusätzlichen Festplattenspeicher zu.

Kapitel 10: Schnelle Problemlösung

In einem Netzwerk können durch die kleinsten Probleme eine ganze Reihe von Services und Funktionen betroffen sein. Netzwerkmanagement-Systeme erkennen diese Probleme und sind häufig in der Lage, Ereignisströme auszusenden, um Leistungsabnahmen, Ausfälle und beeinträchtigte Services zu melden. Diese Fülle an Informationen, wenn sie auch genau ist, behindert häufig die Problembehebungsanstrengungen aufgrund der großen Datenmenge, die der Bediener filtern muss.

Mit der Netzwerk- und Sprachmanagementlösung von CA können Sie Ihre Problembehebungsanstrengungen leichter auf die Problemquelle fokussieren. Die SPECTRUM-Software führt eine Korrelation der Ereignisse, eine Auswirkungsanalyse und RCA für mehrere Anbieter und Technologien über verschiedene Netzwerk-, System-, Sprach- und Anwendungsinfrastrukturen hinweg aus. Durch die Kombination der Fähigkeiten von eHealth, Änderungen des Leistungsverhaltens zu erkennen und zu melden, und der Fähigkeiten von eHealth for Voice, die Richtlinien und Kapazitäten von Sprachnetzwerken zu überwachen, bietet CA eine Schlüssellösung zur Identifikation von Problemen, die sich schnell auf die eigentliche Quelle des Problems konzentriert und eine tiefere Einsicht in historische Trends und Berichte bietet.

In diesem Kapitel wird beschrieben, wie die Vorgänge zur Problemlösung und Ursachenbestimmung von SPECTRUM funktionieren.

Verfahren zur Problemlösung

SPECTRUM bietet drei intelligente, automatisierte und integrierte Ansätze zur Lösung von Problemen:

- Modellbasierte IMT
- Regelbasiertes EMS
- Richtlinienbasierte Technologie zur Korrelation von Bedingungen (Condition Correlation Technology, CCT)

SPECTRUM ist im Grunde ein modellbasiertes System. Modellbasierte Systeme können an Änderungen angepasst werden, die in einer bedarfsorientierten Echtzeit-IT-Infrastruktur regelmäßig anstehen. Regelbasierte Systeme sind so flexibel, dass Kunden ihre eigene Intelligenz integrieren können, ohne dafür über Programmierkenntnisse verfügen zu müssen. SPECTRUM kombiniert die Vorteile beider Ansätze, indem es Modelle einsetzt, um eine flexible Anpassung an Änderungen zu erzielen, und dabei leicht zu erstellende Regeln für das Modell verwendet, so dass kein ständiges Bearbeiten der Regeln erforderlich ist. Richtlinienbasierte Systeme stellen ein automatisiertes Mittel zur Verbindung von scheinbar unzusammenhängenden Informationen zur Bestimmung von Bedingung und Zustand von physischen Geräten und logischen Services dar. Dieses Modul zur Korrelation von Bedingungen bietet in Kombination mit den Modellierungs- und Regelmodulen von SPECTRUM eine höhere Ebene der siloübergreifenden Serviceanalyse.

Fast alle Probleme mit der Servicebereitstellung können in eine der folgenden drei Kategorien eingeteilt werden: Verfügbarkeit, Performance oder überschrittene Schwellenwerte. Infrastrukturfehler treten auf, wenn etwas kaputt geht, ganz gleich, ob sie sich auf LAN/WAN, Server, Speicher, Datenbank, Anwendung oder Sicherheit beziehen. Probleme mit der Performance einer Infrastruktur führen häufig zu Spannungsabfall, so dass Services zwar weiterhin verfügbar sind, jedoch eine schlechte Performance liefern. Aus der Perspektive des Benutzers ist eine langsame Infrastruktur mit einer defekten Infrastruktur gleichzusetzen. Zur letzten Kategorie gehört ungewöhnliches Verhalten, bei dem Performance-, Verwendungs- oder Kapazitätsschwellenwerte überschritten wurden, wenn Bedarfs-/Lastfaktoren erheblich über die beobachteten Baselines stiegen bzw. darunter fielen.

SPECTRUM, eHealth und eHealth for Voice können diese Probleme in Ihrem Netzwerk erkennen und Alarme ausgeben, wenn Probleme auftreten. Da alle Alarme an SPECTRUM gesendet werden, können Sie die Ursachen von Problemen ausmachen.

Modellbasierte, regelbasierte und richtlinienbasierte Analysen in SPECTRUM erkennen die Beziehungen zwischen Elementen der IT-Infrastruktur und den Kunden- oder Geschäftsprozessen, für deren Unterstützung sie konzipiert sind. Durch dieses Erkennen von Beziehungen konnte SPECTRUM eine 70-prozentige Reduzierung von Ausfallzeiten erzielen und 90 % der Verfügbarkeits- oder Performanceprobleme von einem zentralen Standort aus lösen. Durch die RCA von SPECTRUM konnte die Anzahl von Alarmen um ein Vielfaches gesenkt und die MTTR von Stunden auf Minuten reduziert werden. Die verteilte Managementarchitektur von SPECTRUM hat sich auch zur Ausführung der RCA für über 5 Millionen Geräte (über 20 Millionen Ports) in einer einzigen Umgebung mit vollständig vernetzten und redundanten Kern- und Verteilungsnetzwerkschichten als effektiv erwiesen. Durch unseren integrierten Ansatz zum Fehler- und Performancemanagement können Unternehmen, Regierungen und Serviceanbieter auf der ganzen Welt wichtige Managementaufgaben durch Service-Level-Erkennung ausführen.

Komplexe Probleme und leistungsfähige Lösungen

Das Betriebsmanagement in einer IT-Infrastruktur ist ein schwieriges, ressourcenintensives und doch notwendiges Unterfangen. Wenn die Infrastruktur zusammenbricht oder langsamer wird, sind Tools erforderlich, um die Ursache schnell auszumachen, alle symptomatischen Fehler zu unterdrücken, auf der Grundlage der Auswirkungen auf das Geschäft Prioritäten zu setzen sowie bei der Problembehebung und bei Reparaturen Hilfestellung zu leisten, um die Wiederherstellung des Services zu beschleunigen.

Zur Sicherstellung der Performance und der Verfügbarkeit einer Infrastruktur verfolgen die meisten Unternehmen einen doppelten Ansatz mit hochverfügbaren, fehlertoleranten, lastausgleichenden Designs für Infrastrukturgeräte und Kommunikationspfade sowie eine Managementlösung zur Gewährleistung eines ordnungsgemäßen Betriebs. Die Aufgaben der Managementlösung werden zusätzlich durch die heutigen Hochverfügbarkeitsumgebungen verkompliziert. Die Managementlösung muss die Lastausgleichskapazität verstehen sowie primäre und fehlertolerante Sicherungspfade nachverfolgen und erkennen, wann redundante Systeme aktiv sind. Die Investition in die Managementlösung ist genauso wichtig wie die Investition in die Infrastruktur an sich.

Vorhersage von Problemen und Vermeidung

Mit einer Management-Software können Probleme besser vorhergesagt bzw. vermieden werden. Die von CA vordefinierten Schwellenwerte für Auslastung, Performance und Antwortzeit können als Frühwarnsystem fungieren, wenn ein Problem oder eine Verletzung der Service-Level-Gewährleistung kurz bevorsteht. Diese Schwellenwerte können natürlich an die spezifische Umgebung des Kunden angepasst werden, es ist jedoch auch wichtig, dass gleich zu Beginn der Überwachungs-Baselines fertig definierte Schwellenwerte vorhanden sind.

Bevor Sie mit der eigentlichen Fehlerbehebung beginnen können, müssen Sie das Problem ausfindig machen. Es reicht nicht aus, sich des Problems bewusst zu sein und Daten dazu zu sammeln. Um das Problem effektiv behandeln zu können, müssen Sie den Ort oder die Quelle des Problems finden und darüber hinaus auch ermittelt, wo das Problem nicht besteht. Wenn mehrere Probleme gleichzeitig auftreten, müssen Sie in der Lage sein, die Probleme automatisch auf der Grundlage der betroffenen Kunden, Services oder Infrastrukturgeräte nach Priorität zu ordnen. Es ist viel zu kostspielig, sich bei der Bestimmung der Ursache von Problemen allein auf menschliches Eingreifen zu verlassen und dabei den unendlichen Strom an symptomatischen Problemen durchzuarbeiten. Jede Minute Arbeit zur Isolierung des Problems ist eine Minute weniger für die Lösung des Problems.

Auswirkungen auf das Unternehmen

Die besten Managementlösungen sind nicht nur in der Lage, Probleme zu erkennen, diese zu isolieren und alle symptomatischen Ereignisse zu unterdrücken, sondern auch, alle betroffenen Komponenten, Services und Kunden zu identifizieren. Für das Unternehmen ist es wichtig, sowohl die Auswirkungen zu verstehen als auch die Ursache zu finden. Bei Ausfällen oder Leistungseinbußen sind Unternehmensservices und deren Benutzer betroffen. In solchen Fällen können Mitarbeiter normalerweise nicht wirtschaftlich arbeiten, d. h., die Produktivität sowie die Effizienz leiden. Manchmal sind auch die Services betroffen, die das Unternehmen seinen Kunden zur Verfügung stellt, was zu entgangenen Einnahmen, SLA-Strafen und im schlimmsten Fall zum Kundenverlust führt.

Bei großen Organisationen kann es vorkommen, dass viele Probleme gleichzeitig auftreten. Durch Kenntnis der Ursache eines Problems können Organisationen Probleme schnell und effizient lösen, ohne Zeit mit der Symptombekämpfung zu verschwenden. Wenn die Auswirkungen von Problemen bekannt sind, kann das Unternehmen bei deren Behebung Prioritäten setzen und effektive Unterstützung durch die Helpdesk-Services leisten.

Ereigniskorrelation und RCA – Ein dreiteiliger Ansatz

Die Analyse der Ursachen in SPECTRUM (Root Cause Analysis, RCA) basiert auf den folgenden Grundsätzen:

- Das System muss die Beziehung zwischen Informationen innerhalb der Infrastruktur einerseits und den Systemen/Anwendungen/Services/Kunden andererseits verstehen, die diese Informationen benötigen.
- Das System muss bei der Überwachung proaktiv vorgehen anstatt auf Ereignisströme zurückzugreifen.
- Das System muss zwischen einer Fülle von Ereignissen und aussagekräftigen Alarmen unterscheiden.
- Das System muss skalierbar sein und sich an die Anforderungen wachsender und dynamischer Infrastrukturen anpassen.
- Die Lösung muss mit Lösungen verschiedener Anbieter und Technologien funktionieren.
- Das System muss für Erweiterungen und Anpassungen geeignet sein.

Management-Softwareprogramme, die RCA auf effiziente Weise ausführen, sollten einen Alarm für die Hauptbedingung auslösen und verhindern, dass jegliche Symptome/Auswirkungen der Hauptbedingung als ein eindeutiger oder separater Alarm ausgegeben werden.

SPECTRUM setzt zur Ereigniskorrelation und für die RCA-Funktionen mehrere kooperativ arbeitende Verfahren ein. Dazu gehören IMT, EMS und CCT. Diese Verfahren dienen zur Diagnose einer Vielfalt von verschiedenen, oft unvorhersehbaren Problemen.

RCA

RCA besteht im Grunde aus dem Interpretieren einer Gruppe von Symptomen/Ereignissen und aus dem Bestimmen ihrer Ursache. Im Kontext des Infrastrukturmanagements sind Ereignisse Vorkommen von bedeutenden Geschehnissen, die von einer Quelle an andere Systeme bekannt gegeben werden. Ereignisse treten normalerweise in der Quelle lokal auf und helfen ohne den entsprechenden Kontext nicht immer bei der RCA weiter.

Häufig ist die Ereigniskorrelation erforderlich, um zu bestimmen, ob aktionsfähige Bedingungen oder Probleme vorliegen. Um Probleme zu isolieren, alle betroffenen Komponenten und Services zu identifizieren und alle symptomatischen Ereignisse zu unterdrücken, ist die Ereigniskorrelation jedoch unumgänglich. Viele Komponenten geben Ereignisse in verschiedenen Formaten aus: SNMP-Traps, Syslog-Meldungen, Einträge in die Anwendungsprotokolldatei, TL1-Ereignisse, ASCII-Streams usw. Modernere Management-Systeme wie SPECTRUM, eHealth und eHealth for Voice können Ereignisse auch auf der Grundlage von proaktiven Abfragen des Komponentenstatus, parameterbasierten Grenzwertüberschreitungen, Grenzwertüberschreitungen bei der Antwortzeitmessung, Abweichungen vom üblichen Leistungsverlauf sowie der Health-Analyse generieren.

Die RCA von SPECTRUM ist ein automatisiertes Verfahren zur Behandlung von Problemen mit der Infrastruktur und zur Identifizierung von verwalteten Elementen, die ihre Funktion nicht erfüllen. Das Ziel der RCA von SPECTRUM lässt sich ganz einfach ausdrücken als das Identifizieren einer einzelnen Fehlerquelle, der Ursache, und das Erstellen des entsprechenden aktionsfähigen Alarms für das fehlerhafte verwaltete Element.

Verfahren zur induktiven Modellierung

Der Kern der RCA-Lösung von SPECTRUM ist das patentierte IMT. IMT verwendet ein leistungsstarkes objektorientiertes Modellierungsparadigma mit modellbasierten Folgerungsanalytiken. IMT wird in SPECTRUM meist zur Analyse der physischen und logischen Topologie eingesetzt, da SPECTRUM mit Hilfe der Auto-Discovery-Engine topologische Beziehungen automatisch zuordnen kann.

In SPECTRUM wird die Softwaredarstellung eines echten verwalteten Elements oder einer Komponente dieses Elements als „Modell“ bezeichnet. Durch diese Darstellung kann SPECTRUM nicht nur einzelne Elemente im Netzwerk untersuchen und abfragen, sondern auch die Mittel zum Aufbau einer Beziehung zwischen Elementen bereitstellen, um diese als Teil eines größeren Systems zu erkennen. Die RCA des IMT basiert auf einem komplexen System von Modellen, Beziehungen und Verhalten, die eine Softwaredarstellung der Infrastruktur bilden. Die Entscheidungen, welche Elemente fehlerhaft sind, werden nicht anhand eines einzelnen Elements getroffen. Stattdessen werden die Beziehungen zwischen den Elementen betrachtet und die Zustände der zusammengehörigen verwalteten Elemente in die Analyse einbezogen. Modelle kommunizieren direkt mit ihren echten Gegenständen, so dass SPECTRUM diese nicht nur überwachen, sondern auch proaktiv den Zustand oder zusätzliche Diagnoseinformationen abfragen kann. Modelle werden anhand ihrer Attribute, ihres Verhaltens, ihrer Beziehungen zu anderen Modellen und ihrer algorithmischen Intelligenz beschrieben.

Die intelligente Analyse wird durch die Zusammenarbeit von Modellen in einem System möglich. Diese Zusammenarbeit ermöglicht die Korrelation der Symptome, die Unterdrückung von unnötigen Alarmen und die Auswirkungsanalyse von betroffenen Benutzern, Kunden und Services. Durch Zusammenarbeit besteht die Möglichkeit zum Austausch von Informationen und zum Starten der Verarbeitung zwischen beliebigen Modellen im Modellierungssystem. Ein Modell, das eine Anforderung an ein anderes Modell stellt, kann im Gegenzug als Auslöser dafür sorgen, dass dieses Modell Anforderungen an andere Modelle stellt usw. Beziehungen zwischen Modellen lassen den Kontext für die Zusammenarbeit entstehen.

Durch Zusammenarbeit zwischen Modellen wird Folgendes möglich:

- Korrelation der Symptome
- Unterdrückung von unnötigen/symptomatischen Alarmen
- Auswirkungsanalyse

Ein einfaches Einsatzbeispiel für IMT ist der Übergang des Netzwerkrouterports von UP nach DOWN. Wenn ein Portmodell einen LINK-DOWN-Trap empfängt, verfügt es über die nötige Intelligenz, um durch eine Statusabfrage bestimmen zu können, ob der Port tatsächlich DOWN ist. Ist der Port tatsächlich ausgefallen (DOWN), wird das System der Modelle hinzugezogen, um zu bestimmen, ob der Port über Lower-Layer-Sub-Interfaces verfügt. Wenn eins oder mehrere der Lower-Layer-Sub-Interfaces auch DOWN sind, wird nur die Bedingung des Ports in der unteren Schicht als Alarm ausgegeben. Ein Anwendungsbeispiel hierzu ist der Übergang mehrerer Frame Relay-DLCIs in den Status INACTIVE. Wenn der Frame Relay-Port DOWN ist, unterdrückt IMT die symptomatischen Bedingungen „DLCI INACTIVE“ und löst einen Alarm für das Frame Relay-Portmodell aus. Wenn darüber hinaus die Portübergänge DOWN sind, fragt das IMT den Status der angeschlossenen Netzwerkelemente (NEs) ab, und wenn diese auch DOWN sind, werden diese Bedingungen als Symptom des Portstatus DOWN betrachtet und unterdrückt und sind vom Alarm zum Portstatus DOWN betroffen. Ursache und Auswirkung werden mit Hilfe der Fähigkeit des IMT zum Überwachen der Infrastruktur und Kommunizieren mit der Infrastruktur bestimmt.

Das Ereignis-Management-System

Zu bestimmten Zeiten sind die lokalen Ereignisströme einer bestimmten Quelle die einzige Quelle für Managementinformationen. Jedes beliebige Ereignis kann ein wichtiges Geschehen sein, muss es aber nicht. Im Kontext anderer Ereignisse, Informationen oder Zeiträume kann es eine aktionsfähige Bedingung darstellen. Ereignisregeln im Ereignis-Management-System von SPECTRUM stellen ein breit gefächertes Entscheidungsfindungssystem bereit, mit dem angezeigt werden kann, wie Ereignisse verarbeitet werden müssen. Sie können Ereignisregeln anwenden, um nach einer Reihe von Ereignissen zu suchen, die in einem Modell in einem bestimmten Muster, in einem bestimmten Zeitrahmen oder mit bestimmten Datenwertbereichen auftreten. Mit Ereignisregeln können andere Ereignisse und sogar Alarme erstellt werden.

Wenn Ereignisse auftreten, die die Vorbedingungen einer Regel erfüllen, kann SPECTRUM folgende Aktionen ausführen:

- Erstellen eines weiteren Ereignisses, so dass sich die Ereignisse überlappen.
- Protokollieren des Ereignisses zur späteren Berichterstellung/Problembehandlung.
- Heraufstufen des Ereignisses zu einem aktionsfähigen Alarm.

SPECTRUM stellt sechs benutzerdefinierbare Ereignisregeltypen bereit, die die Grundlage der regelbasierten Ereignis-Management-System-Engine bilden.

Diese Regeltypen sind Bausteine, die einzeln oder gemeinsam eingesetzt werden können, um einen Alarm für die einfachsten oder die komplexesten ereignisorientierten Szenarien einzurichten. Mit dieser Regel-Engine des Ereignis-Management-Systems ist die Korrelation von Ereignisfrequenz/-dauer, Ereignisabfolge und Ereigniskopplung möglich.

Folgende Typen von Ereignisregeln stehen zur Verfügung:

- **Ereignispaar (Ereigniskopplung):** Durch diese Regel wird ein Fehler generiert, wenn das erste von zwei von Ihnen definierten Ereignissen nicht in der angegebenen Reihenfolge eintritt. Tritt das zweite Ereignis in einer Serie nicht ein, kann ein Fehler vorliegen. Der Regeltyp „Ereignispaar“ erstellt ein für dieses Szenario relevanteres Ereignis. Durch Ereignisregeln, die zum Regeltyp „Ereignispaar“ gehören, wird ein neues Ereignis erstellt, wenn ein Ereignis ohne das mit ihm gepaarte Ereignis eintritt. Es können andere Ereignisse zwischen gepaarten Ereignissen eintreten, ohne dass dies Auswirkungen auf diese Ereignisregel hat.

- **Ereignisratenzähler (Ereignisfrequenz):** Dieser Regeltyp erstellt ein neues Ereignis, wenn Ereignisse mit einer bestimmten Frequenz in einer bestimmten Zeitspanne eintreten. Wenige Ereignisse eines bestimmten Typs stellen eventuell kein Problem dar, aber wenn die Anzahl dieser Ereignisse einen bestimmten Schwellenwert in einer bestimmten Zeitspanne übersteigt, ist eine Benachrichtigung erforderlich. SPECTRUM erstellt keine zusätzlichen Ereignisse, wenn die Rate oberhalb des Schwellenwerts liegt. Fällt die Rate zuerst unter den Schwellenwert und steigt anschließend wieder über diesen Wert an, wird ein weiteres Ereignis generiert. Der Typ „Ereignisratenzähler“ ist am besten zur Erkennung einer lang anhaltenden Häufung von Ereignissen geeignet.
- **Ereignisratenfenster (Ereignisfrequenz):** Dieser Regeltyp generiert ein neues Ereignis, wenn mehrere gleiche Ereignisse über einen angegebenen Zeitraum hinweg generiert werden. Der Typ „Ereignisratenfenster“ ist am besten dazu geeignet, kürzere Häufungen von Ereignissen zu erkennen. Er überwacht ein Ereignis, das zwar bei gelegentlichen Vorkommen nicht bedeutend, jedoch bei vielen Vorkommen in einer kurzen Zeitspanne bedeutend ist. Wenn ein Ereignis einige Male über den Tag verteilt auftritt, liegt möglicherweise kein Problem vor. Tritt ein Ereignis jedoch fünf Mal in einer Minute auf, liegt eventuell ein Zustand vor, über den Sie benachrichtigt werden möchten. Übersteigt die Anzahl der Vorkommen eines Ereignisses eine bestimmte Frequenz, generiert SPECTRUM ein weiteres Ereignis. SPECTRUM erstellt keine zusätzlichen Ereignisse, wenn die Frequenz oberhalb des Grenzwerts liegt. Fällt die Rate zuerst unter den Schwellenwert und steigt anschließend wieder über diesen Wert an, wird ein weiteres Ereignis generiert.
- **Ereignisabfolge (Ereignisabfolge)** Dieser Regeltyp generiert ein Ereignis, wenn eine bestimmte Reihenfolge von Ereignissen einer Abfolge in der betreffenden Umgebung bedeutend sein könnte. In dieser Abfolge kann eine beliebige Anzahl und jeder Typ von Ereignis vorkommen. Wenn die Abfolge in der angegebenen Zeitspanne erkannt wird, generiert SPECTRUM ein neues Ereignis.
- **Ereigniskombination (Ereigniskopplung):** Dieser Regeltyp generiert ein neues Ereignis, wenn eine bestimmte Kombination von Ereignissen in einer beliebigen Reihenfolge auftritt. Die Kombination kann eine beliebige Ereignisanzahl und jeden Typ von Ereignis umfassen. Wenn die Kombination in einer angegebenen Zeitspanne erkannt wird, generiert SPECTRUM ein neues Ereignis.
- **Ereignisbedingung (Ereigniskopplung):** Dieser Regeltyp generiert ein Ereignis auf der Grundlage eines konditionalen Ausdrucks. SPECTRUM setzt das Prinzip „Vertrauen ist gut, Kontrolle ist besser“ ein: eine Reihe von konditionalen Ausdrücken kann in der Ereignisregel aufgelistet werden, und der erste Ausdruck, der als TRUE gilt, wird das in der Bedingung angegebene Ereignis generieren. Sie können Regeln erstellen, um durch das kombinierte Auswerten von Ereignisdaten und IMT-Modelldaten (einschließlich Attributen, die direkt aus dem remote verwalteten Element gelesen werden) Korrelation herzustellen. Wenn beispielsweise ein Trap empfangen wird, der das Management-System über die Überlastung des Arbeitsspeicherpuffers benachrichtigt, kann eine Ereignisbedingungsregel das Senden einer Anforderung an das Gerät auslösen, um die tatsächliche Speicherauslastung zu überprüfen und somit festzustellen, ob wirklich eine Alarmbedingung vorliegt.

SPECTRUM implementiert eine Reihe von fertigen Ereignisregeln, indem es ein oder mehrere Ereignisregeltypen auf Ereignisströme anwendet. Ereignisregeln können mit Hilfe beliebiger Regeltypen erstellt oder angepasst und auf andere Ereignisströme angewendet werden. Auf die Implementierung von Ereignisregeln über das Ereignis-Management-System wird später in diesem Dokument ausführlicher eingegangen.

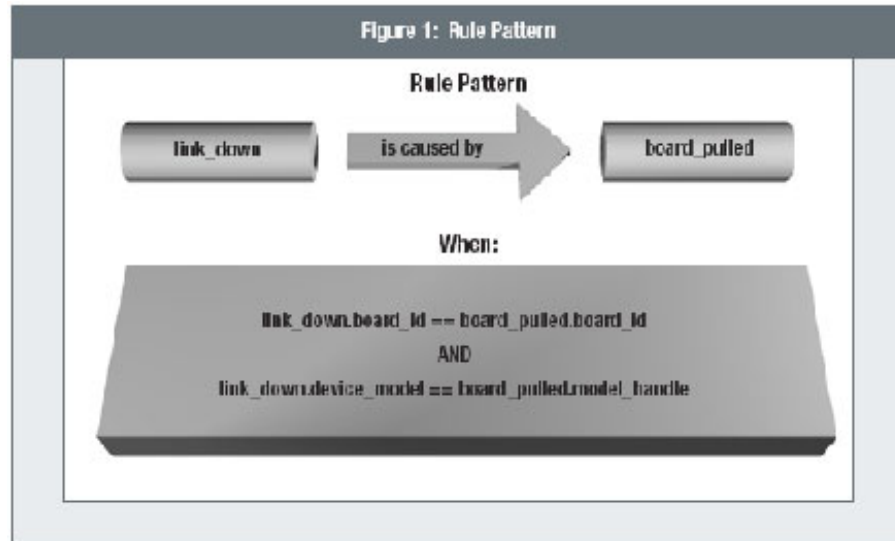
Korrelation der Bedingungen

Zur Durchführung komplexerer benutzerdefinierter oder benutzergesteuerter Korrelationen stellt SPECTRUM eine richtlinienbasierte CCT bereit, mit der folgende Aufgaben ausgeführt werden können:

- Erstellung von Korrelationsrichtlinien
- Erstellung von Korrelationsdomänen
- Korrelation von scheinbar ungleichen Ereignisströmen und Bedingungen
- Korrelation zwischen Sets von verwalteten Elementen
- Korrelation in verwalteten Domänen
- Korrelation zwischen Sets von verwalteten Domänen
- Korrelation von Komponentenbedingungen, wie sie höheren Auftragskonzepten wie Unternehmensservices oder Kundenzugriff zugeordnet sind

Einige wichtige Konzepte beziehen sich auf die Bedingungskorrelation:

- **Bedingungen:** Eine Bedingung ähnelt einem Zustand. Durch ein Ereignis/eine Aktion kann eine Bedingung festgelegt sowie gelöscht werden. Es ist auch möglich, dass eine Bedingung durch ein Ereignis festgelegt wird, aber für das Aufheben dieser Bedingung eine Aktion des Benutzers erforderlich ist. Die Bedingung besteht ab dem Zeitpunkt, zu dem sie festgelegt wird, und bis zu dem Zeitpunkt, zu dem sie aufgehoben wird. Ein sehr einfaches Beispiel für eine Bedingung ist die Bedingung „Port down“. Diese Bedingung gilt ausschließlich für ein bestimmtes Interface ab dem Zeitpunkt, zu dem der LINK-DOWN-Trap oder das Ereignis zum Festlegen (z. B. eine fehlgeschlagene Statusabfrage) empfangen wird, bis zu dem Zeitpunkt, zu dem der LINK-UP-Trap oder das Löscheignis (z. B. eine erfolgreiche Statusabfrage) empfangen wird. Eine Reihe von Bedingungen, die zum Herstellen von Korrelationen auf Domänenebene hilfreich sein können, sind in SPECTRUM vordefiniert, und es können weitere hinzugefügt werden.
- **Scheinbar ungleiche Bedingungen:** Viele Geräte in einer IT-Infrastruktur bieten eine bestimmte Funktion. Die Funktion auf Geräteebene ist häufig kontextlos, da sie mit Funktionen von anderen Geräten/Komponenten zusammenhängt. Die meisten verwalteten Elemente können Ereignisströme ausgeben, aber diese Ereignisströme gelten lokal für die einzelnen Komponenten. Ein einfaches Beispiel hierfür wäre, wenn ein Antwortzeitmanagement-System eine Bedingung für ein Testergebnis identifiziert, das einen Schwellenwert übersteigt. Gleichzeitig kann ein Elementverwaltungssystem die Bedingung bestimmen, wenn ein Routerport einen Schwellenwert für die Übertragungsbandbreite übersteigt. Diese Bedingungen sind scheinbar ungleich, da sie unabhängig voneinander und ohne Kontext oder Wissen voneinander erstellt wurden. Tatsächlich hängen die beiden Bedingungen jedoch häufig zusammen, d. h., ein überlasteter Port könnte die Ursache für den Antwortleistungsabfall sein.
- **Regelmuster:** Regelmuster ordnen Bedingungen zu, wenn bestimmte Kriterien erfüllt werden. Ein einfaches Beispiel ist die Bedingung „Port ausgefallen“, die durch die Bedingung „Karte entnommen“ entsteht. Die zwei Bedingungen hängen wahrscheinlich zusammen, wenn der Port und die Karte die gleiche Steckplatznummer aufweisen. Das folgende Diagramm stellt dieses Regelmuster dar. Ein Regelmuster kann zur Erzeugung eines aktionsfähigen Alarms oder zur Unterdrückung von symptomatischen Alarmen dienen.



- **Korrelationsdomänen:** Mit einer Korrelationsdomäne kann der Umfang von einer oder mehreren Korrelationsrichtlinien sowohl definiert als auch eingeschränkt werden. Sie kann auf einen bestimmten Service angewendet werden. In der Kabelbreitbandumgebung beispielsweise können Rückleitungsfehler in einem bestimmten geografischen Servicebereich durch ein Rückleitungsüberwachungssystem erkannt werden. Diese „Rückleitungsfehler“-Bedingung hat zur Folge, dass Hochgeschwindigkeitskabelmodems von Abonnenten unerreichbar werden und Video on Demand (VoD) Pay-Per-View-Streams fehlschlagen. Das Wissen, dass sich der Rückleitungsfehler, die Modemprobleme und die fehlgeschlagenen Videostreams alle in der gleichen Korrelationsdomäne befinden, ist für die Korrelation der Ereignisse und letztendlich zur Identifizierung der Ursache entscheidend. Es ist ebenfalls sehr wichtig, bestimmen zu können, dass eine „Rückleitungsfehler“-Bedingung, die in einer Korrelationsdomäne (Philadelphia) auftritt, nicht mit VoD-Streamfehlerbedingungen in einer anderen Korrelationsdomäne (New York) korreliert werden darf.
- **Korrelationsrichtlinien:** Es können mehrere Regelmuster in Korrelationsrichtlinien gebündelt werden. Anschließend können Sie die Korrelationsrichtlinien auf einen Service oder eine Korrelationsdomäne anwenden. Sie können beispielsweise ein Bündel von Regelmustern erstellen, das für OSPF gilt, und dieses als OSPF-Korrelationsrichtlinie bezeichnen. Die OSPF-Korrelationsrichtlinie kann auf die einzelnen Korrelationsdomänen angewendet werden, wobei die einzelnen unabhängigen OSPF-Regionen und die unterstützenden Router in dieser Region die Korrelationsdomäne definieren. Ein weiteres Beispiel wäre, wenn Sie eine Korrelationsrichtlinie auf der Grundlage einer Gruppe von Regelmustern definieren, die innerhalb eines MPLS/BGP-VPN operieren, bezeichnet als Intra-VPN-Richtlinie, und diese auf alle modellierten VPNs übertragen. Wenn einer Korrelationsrichtlinie eine Regel hinzugefügt bzw. wenn eine Regel daraus entfernt wird, aktualisiert SPECTRUM sofort automatisch alle betroffenen Korrelationsdomänen. Auf einzelne Korrelationsdomänen können mehrere Korrelationsrichtlinien angewendet werden, und im Gegenzug kann eine Korrelationsrichtlinie auf viele Korrelationsdomänen angewendet werden.

Bedingungs-basierte Korrelationen sind sehr leistungsstark und bieten einen Mechanismus zur Entwicklung von Korrelationsrichtlinien und deren Anwendung auf Korrelationsdomänen. Wenn Sie diese auf das Service-Level-Management anwenden, ähneln Korrelationsrichtlinien den Metriken eines SLA, und Korrelationsdomänen ähneln Service, Kunde oder geografischen Gruppierungen. Gelegentlich ist es nur möglich, eine kausale Beziehung zwischen zwei oder mehr scheinbar ungleichen Bedingungen abzuleiten, wenn diese Bedingungen in einer gemeinsamen Korrelationsdomäne auftreten. Diese Mechanismen sind notwendig, wenn SPECTRUM durch Abfragen keine kausalen Beziehungen feststellen kann.

Fehlerszenarien

SPECTRUM kann in der Ausgangseinstellung auf viele verschiedene Szenarien eingehen und für diese eine RCA durchführen. In diesem Abschnitt finden Sie bestimmte Szenarien, in denen die im vorherigen Abschnitt beschriebenen Techniken angewendet werden, um eine RCA und die Auswirkungsanalyse auszuführen. Um die Erläuterungen kurz und einfach zu halten, werden lediglich die Details der grundlegenden Bearbeitung genannt. Die folgende Tabelle enthält zu Anschauungszwecken die Farben von Alarmen, die der Symbolstatus von SPECTRUM-Modellen aufweisen kann.

Status des Modells	Farbe des Alarms
Normalbetrieb	GRÜN
Kritischer Fehler	ROT
Schwerwiegender Fehler	ORANGE
Geringfügiger Fehler	GELB
Unbekannt oder Unterdrückt	GRAU
Inaktiv aus Wartungsgründen	BRAUN
Anfangszustand	BLAU

Kommunikationsausfälle und deren Auswirkungen

Kommunikationsausfälle gehören zu den Fehlertypen, die häufig als „Blackouts“ oder „schwerwiegende Fehler“ bezeichnet werden. Bei diesen Fehlertypen ist mindestens ein Kommunikationspfad so stark belastet, dass kein Datenverkehr mehr möglich ist. Der Fehler kann viele Ursachen haben, z. B. beschädigte Kupferleitungen/Faserkabel/Leitungen, falsch konfigurierte Router/Switches, Hardwarefehler, schwere Performanceprobleme, Sicherheitsbedrohungen usw. Bei diesen schweren Kommunikationsfehlern stehen dem Management-System nur begrenzt Informationen zur Verfügung, da es keine Informationen mit einem oder mehreren verwalteten Elementen austauschen kann. Durch sein ausgefeiltes System aus Modellen, Beziehungen und über IMT verfügbaren Verhalten kann SPECTRUM die Fehler und Auswirkungen ableiten. IMT-Ableitungsalgorithmen werden auch als „Inference Handler“ bezeichnet. Eine Gruppe von Inference Handlern, die zu einem bestimmten Zweck entwickelt wurden, werden als Intelligenzkreis oder einfach als Intelligenz bezeichnet.

Isolierung von Kommunikationsausfällen auf Basis der SPECTRUM-Informationen

SPECTRUM bietet leistungsstarke Funktionen, mit denen Sie die eigentlichen Problemquellen im Netzwerk besser aufspüren können. Bei vielen Managementlösungen müssen diese Schritte manuell ausgeführt werden und nehmen sehr viel Zeit in Anspruch. Mit SPECTRUM werden viele dieser Schritte automatisch ausgeführt.

Der Vorgang, über den SPECTRUM Ausfälle identifiziert und isoliert, läuft folgendermaßen ab:

1. Mit SPECTRUM Discovery wird ein Modell Ihrer Infrastruktur erstellt, das die Ressourcen in Ihrem Netzwerk sowie deren Verbindung untereinander darstellt.
2. Bei Empfang eines Problemereignisses überprüft SPECTRUM den Status der eng verbundenen Ressourcen, um zu bestimmen, ob Probleme vorliegen.
3. SPECTRUM analysiert den Status der Ressourcen, um die wahrscheinliche Ursache zu identifizieren.
4. SPECTRUM unterdrückt Alarme, die Symptome der Ursache, aber nicht die Ursache an sich sind.
5. SPECTRUM wertet den Schweregrad des Problems aus, um die Priorität dieses bestimmten Problems unter allen weiteren im Netzwerk gemeldeten Problemen festlegen zu können.

In den folgenden Abschnitten wird diese Funktion von SPECTRUM detaillierter beschrieben.

ERSTELLEN DES MODELLS MIT AUTODISCOVERY

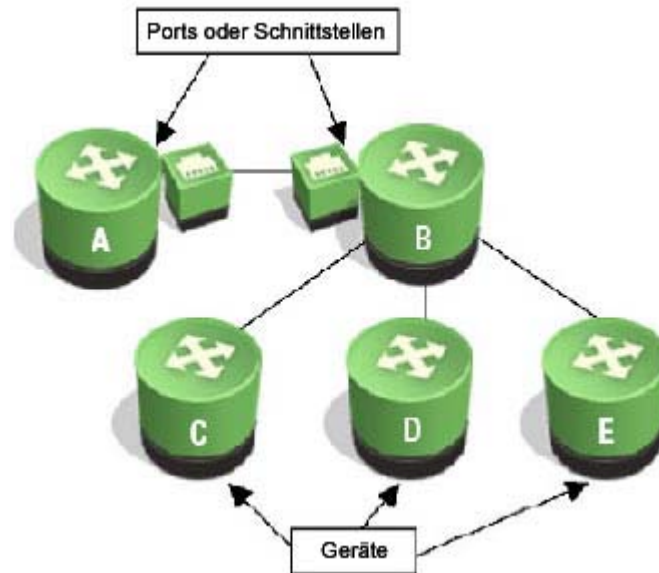
Eine genaue Darstellung der Infrastruktur ist entscheidend, um den Fehler und dessen Auswirkungen zu bestimmen. Das Modellierungssystem von SPECTRUM kann nicht nur eine große Anzahl an Geräten mehrerer Hersteller darstellen, sondern auch eine Vielzahl an Technologien und Verbindungen, die zwischen verschiedenen Infrastrukturelementen vorhanden sein können. SPECTRUM beinhaltet spezielle Lösungen zur Entdeckung von Mehrwegnetzwerken über eine Vielzahl an Technologien, die viele verschiedene Architekturen unterstützen. SPECTRUM bietet Unterstützung für vernetzte und redundante, physische und logische Topologien, die auf ATM, Ethernet, Frame Relay, HSRP, ISDN, ISL, MPLS, Multicast, PPP, VoIP, VPN, VLAN und 802.11 Wireless-Umgebungen oder auch Legacy-Technologien wie FDDI oder Token Ring basieren. Die Modellierung in SPECTRUM ist sehr erweiterungsfähig und kann zum Modellieren der OSI-Layer 1-7 in einer Kommunikationsinfrastruktur eingesetzt werden.

SPECTRUM bietet vier verschiedene Methoden zur Erstellung des Konnektivitätsmodells der physischen und logischen Topologie für jede beliebige Infrastruktur:

- Die SPECTRUM-Anwendung AutoDiscovery fragt die verwaltete Infrastruktur automatisch und dynamisch nach den physischen und logischen Beziehungen ab. Dieser Ansatz von AutoDiscovery wurde im Jahr 1996 patentiert, und SPECTRUM war das erste Produkt, das Layer 2-Switch-Konnektivität erkennen konnte. AutoDiscovery von SPECTRUM arbeitet mit zwei unterschiedlichen Phasen (die Phasen bestehen aus vielen verschiedenen Stufen, die hier jedoch nicht behandelt werden). Die erste Phase besteht aus der Discovery. In dieser Phase (Initiierung in Kapitel 5 beschrieben) erkennt AutoDiscovery automatisch die in der Infrastruktur vorhandenen Elemente. Hierdurch erhält SPECTRUM einen Bestand an Elementen, die verwaltet werden könnten. Die zweite Phase besteht aus der Modellierung. AutoDiscovery setzt Management- und Discovery-Protokolle ein, um die gefundenen Elemente abzufragen und Informationen zu erhalten, über die die Layer 2- und Layer 3-Konnektivität zwischen verwalteten Elementen bestimmt wird. AutoDiscovery führt die Untersuchung von Routing-Tabellen, Bridge-Tabellen und Interfacetabellen beispielsweise über SNMP durch, verwendet aber auch die Verkehrsanalyse sowie herstellereigene Erkennungsprotokolle, z. B. CDP von Cisco. AutoDiscovery ist ein sehr gründlicher, automatisierter Mechanismus zur Erstellung des Infrastrukturmodells.
- Das Modeling Gateway importiert Beschreibungen aller Komponenten der Infrastruktur sowie Informationen zur physischen und logischen Konnektivität aus externen Quellen, z. B. Beschaffungssysteme oder Netzwerktopologiedatenbanken.
- Die Befehlszeilenschnittstelle oder die programmatischen APIs können zum Importieren von Informationen aus externen Quellen eine benutzerdefinierte Integration oder Anwendung erstellen.
- Über die grafische Benutzeroberfläche können Benutzer Modelle auf schnelle Weise durch Zeigen, Klicken und Verschieben per Drag&Drop von Elementen erstellen.

Mit dem Modellierungsschema von SPECTRUM können einzelne verwaltete Elemente logisch in eine beliebige Anzahl von Untermodellen aufgeteilt werden. Diese Sammlung von Modellen und ihre Beziehungen untereinander werden häufig als semantische Datenmodelle für diesen Typ von verwalteten Elementen bezeichnet. Ein typisches semantisches Datenmodell für ein Netzwerkgerät kann daher ein Chassismodell mit Kartenmodellen umfassen, die dem Chassis zugeordnet sind. Physische Interfacemodelle werden den Kartenmodellen zugeordnet. Den einzelnen physischen Interfacemodelle können Gruppen von Sub-Interfacemodelle untergeordnet sein.

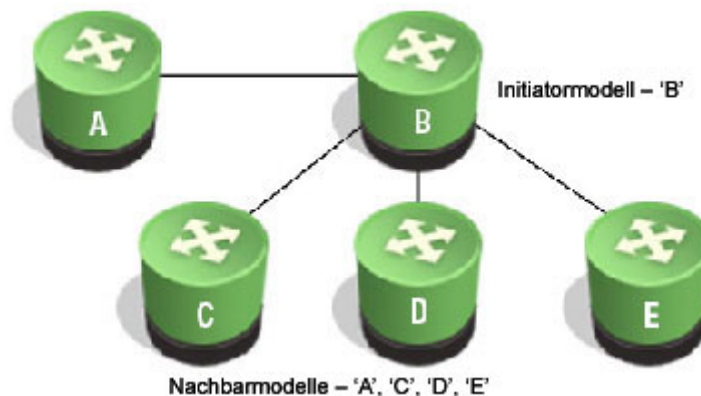
SPECTRUM verfügt über eine Reihe von wohldefinierten Zuordnungen, die festlegen, wie unterschiedliche Gruppen aus semantischen Datenmodellen untereinander agieren. Wenn SPECTRUM die Konnektivität zwischen zwei Geräten darstellt, wird nicht nur zwischen den zwei Ports eine Beziehung hergestellt, die den Link zwischen den beiden bildet, sondern auch zwischen Gerätemodellen und zu den betreffenden Interface- und Portmodellen von anderen Geräten, wie in der folgenden Abbildung dargestellt.



STARTEN DER PROBLEMANALYSE

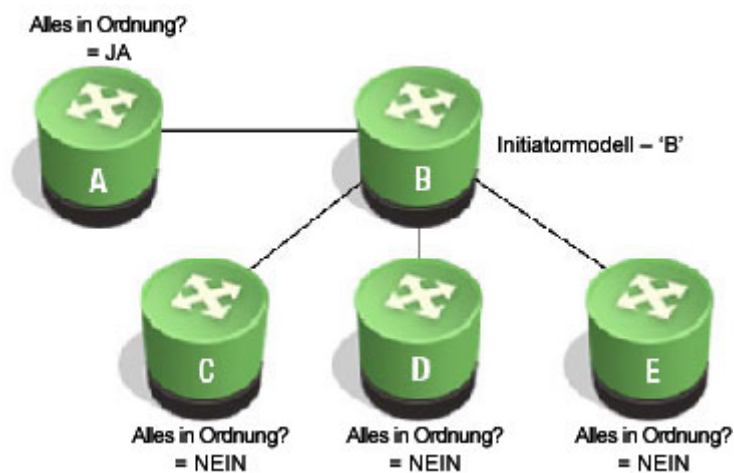
SPECTRUM kann proaktiv mit der Lösung eines Problems beginnen, sobald es ein einziges Symptom empfängt. Es gibt viele Probleme, die die gleichen Symptome aufweisen, SPECTRUM muss jedoch weitere Analysen ausführen, um die Ursache bestimmen zu können. Bei Kommunikationsausfällen beginnt die Analyse, wenn ein Modell in SPECTRUM die Kommunikationsfehler durch fehlgeschlagene Pollings, Traps, Ereignisse, Überschreitungen des Performance-Schwellenwerts oder fehlende Antworten erkennt. SPECTRUM überprüft die Kommunikationsfehler automatisch durch erneute Versuche, alternative Protokolle und Überprüfung von alternativen Pfaden im Rahmen der „Vertrauen ist gut, Kontrolle ist besser“-Methode. Das Modell, in dem das Problem aufgetreten ist, durch das die Intelligenz gestartet wurde, wird als Initiator bezeichnet. Die Intelligenz kann auch durch mehr als ein Modell ausgelöst werden.

Die Initiatormodellintelligenz fordert eine Liste der anderen Modelle an, die direkt damit verbunden sind. Diese verbundenen Modelle werden als Nachbarn des Initiatormodells bezeichnet. Die folgende Abbildung zeigt fünf Modelle, wobei Modell B den Initiator darstellt und die Modelle A, C, D und E seine Nachbarn sind.



Über eine Liste der angegebenen Nachbarn weist die Intelligenz die einzelnen Nachbarmodelle an, den eigenen Status zu überprüfen. Diese Prüfung wird als „Alles in Ordnung?“-Prüfung bezeichnet. „In Ordnung“ ist ein relativer Begriff, und eine eindeutige Gruppe von Attributen, die sich auf Performance und Verfügbarkeit beziehen, sind von Modell zu Modell je nach den tatsächlichen Funktionen des Geräts, das durch das Modell dargestellt wird, unterschiedlich.

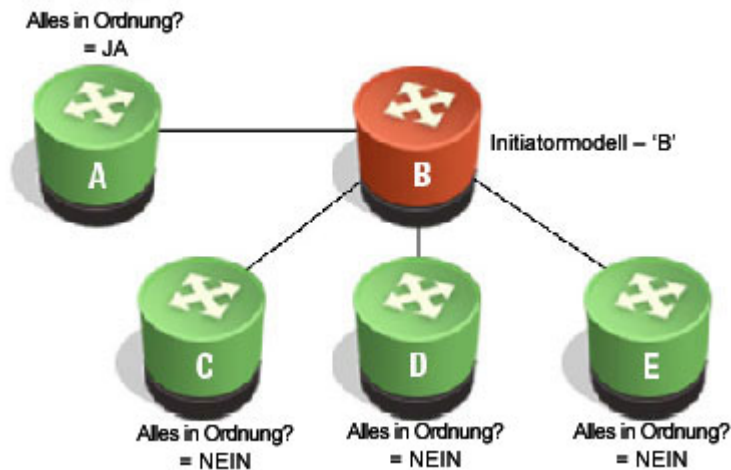
Wenn einem Modell die Frage „Alles in Ordnung?“ gestellt wird, kann das Modell verschiedene Tests/Prüfungen durchführen, um seinen aktuellen Betriebsstatus zu bestätigen. Bei den meisten SNMP-verwalteten Elementen besteht die Prüfung normalerweise aus einer Kombination aus SNMP-Anforderungen, die kann jedoch auch durch Abfragen eines Management Systems oder einfach durch einen ICMP-Ping erfolgen. Eine umfassende Prüfung kann Schwellenwertperformanceberechnungen oder Durchführungen von Antwortzeittests beinhalten.



Die einzelnen Nachbarmodelle beantworten die Frage „Alles in Ordnung?“.

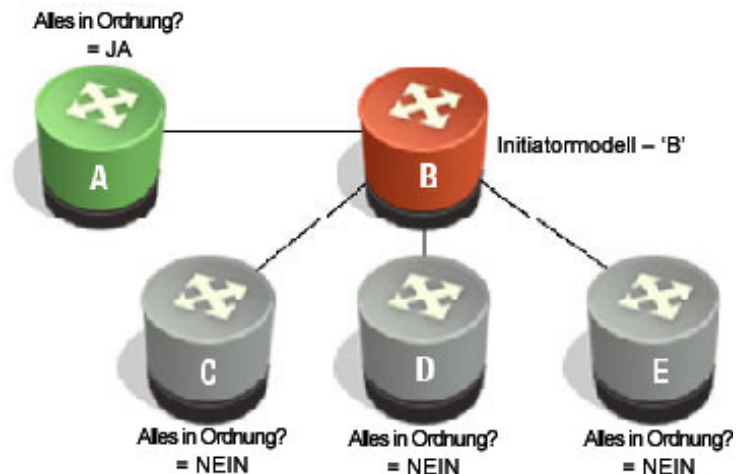
LOKALISIEREN DER URSACHE – FEHLERISOLIERUNG

Wenn das Initiatormodell über einen Nachbarn verfügt, der antwortet, dass alles in Ordnung ist, z. B. Modell A in der vorherigen Abbildung, kann SPECTRUM ableiten, dass das Problem zwischen dem nicht betroffenen Nachbarn und dem betroffenen Initiator (Modell B) liegt. In diesem Fall ist das Initiatormodell, das die Intelligenz ausgelöst hat, wahrscheinlich schuld an diesem Infrastrukturfehler. Daraufhin löst SPECTRUM einen kritischen Alarm für das Initiatormodell aus, der wie in der folgenden Abbildung dargestellt als „Ursachen“-Alarm betrachtet wird.



AUSBLENDEN DER SYMPTOMATISCHEN PROBLEME DURCH ALARMUNTERDRÜCKUNG

Da die Analyse nicht nur aus dem Isolieren des fehlerhaften Geräts (Modell B) besteht, folgt im nächsten Schritt das Analysieren und Unterdrücken der Berichterstellung über die Auswirkungen des Fehlers. Dies ist das Ziel der intelligenten Alarmunterdrückung. Wenn ein Nachbar (z. B. Modell C, D oder E) des Initiatormodells antwortet, dass nicht alles in Ordnung ist, gilt dieser Nachbar als von dem Fehler betroffen, der an einer anderen Stelle der Infrastruktur aufgetreten ist. Daraufhin legt SPECTRUM für diese Modelle den unterdrückten Zustand (Grau) fest, da die Alarmer nur die Symptome eines Problems an einer anderen Stelle darstellen. Die bei diesen Ressourcen auftretenden Probleme sind jedoch nicht die Ursache, und sie liegen wahrscheinlich nur so lange vor, bis die Probleme in Modell B behandelt wurden.



PRIORISIEREN VON PROBLEMEN – ANALYSE DER AUSWIRKUNGEN

SPECTRUM analysiert weiterhin die vollständigen Auswirkungen des Fehlers, da es versteht, dass die einzelnen Modelle Teil eines größeren Netzwerks aus Modellen sind, das die verwaltete Infrastruktur darstellt.

Die Intelligenz analysiert die einzelnen Fehlerdomänen, die aus einer Sammlung von Modellen mit unterdrückten Alarmen bestehen, die zum gleichen Fehler gehören. Diese betroffenen Modelle sind zur Darstellung und Analyse mit dem Hauptfehler verlinkt. Die Intelligenz ermöglicht eine Messung der Auswirkungen dieses Fehlers, indem es die Modelle in der Fehlerdomäne untersucht und ein Maß berechnet, das als Auswirkungsgrad dient. Der Auswirkungsgrad stellt ein Rangsystem dar, damit Bediener die relativen Auswirkungen der einzelnen Infrastrukturfehler schnell auswerten können, um die korrigierenden Aktionen priorisieren zu können.

Das Ereignis-Management-System

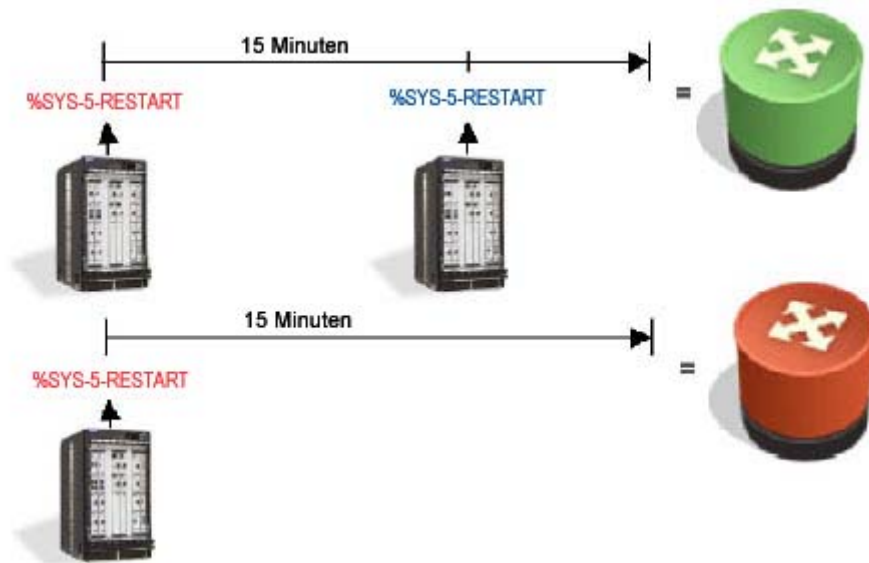
Ereignisregeln ermöglichen eine bessere Bearbeitung und Korrelation von Ereignisströmen. Die Bearbeitung von Ereignisregeln ist dann erforderlich, wenn der Ereignisstrom die einzige Quelle für Management-Informationen ist. Das Southbound Gateway von SPECTRUM beispielsweise ermöglicht das Annehmen von Ereignisströmen von Geräten und Anwendungen, die nicht direkt von SPECTRUM überwacht werden, z. B. eHealth for Voice-PBX-Geräte und Nachrichtenserver. Die intelligente Bearbeitung von Ereignissen in bestimmten Kontexten kann auch über Ereignisregeln (Frequenz, Abfolge, Kombination) erfolgen. Wie bereits zuvor in diesem Kapitel beschrieben, stehen Ihnen sechs Ereignisregeltypen zur Verfügung:

- Ereignispaar: Erwartetes Ereignispaar oder fehlendes Ereignispaar in einer angegebenen Zeitspanne.
- Ereignisratenzähler: Ereignisse mit einer festgelegten Frequenz in einer festgelegten Zeitspanne
- Ereignisratenfenster: Anzahl der Ereignisse in einer angegebenen Zeitspanne
- Ereignisabfolge: Geordnete Abfolge von Ereignissen in einer angegebenen Zeitspanne
- Ereigniskombination: Zwei oder mehr Ereignisse, beliebige Reihenfolge in einer angegebenen Zeitspanne
- Ereignisbedingung: Ereignisse, die auf bestimmte Daten analysiert werden, um das Generieren neuer Ereignisse auf der Grundlage von Vergleichen von variablen Bindungen, Attributen, Konstanten usw. zu ermöglichen

SPECTRUM beinhaltet viele vordefinierte Ereignisregeln, bietet aber auch viele leicht anzuwendende Methoden zur Erstellung von neuen Regeln mit einem oder mehreren Ereignisregeltypen. In diesem Abschnitt werden eine Reihe von vordefinierten Ereignisregeln sowie einige Anwendungsbeispiele für Ereignisregeln vorgestellt.

VORDEFINIIERTE EREIGNISPAARREGEL

SPECTRUM kann Cisco-Syslog-Meldungen als Ereignisströme interpretieren. Die einzelnen Syslog-Meldungen werden im Auftrag von einem verwalteten Switch oder Router generiert und an das SPECTRUM-Modell geleitet, das das entsprechende verwaltete Element darstellt. Eine der vielen Cisco-Syslog-Meldungen gibt an, dass eine neue Konfiguration in den Router geladen wurde. Auf die Reload-Meldung muss immer eine Restart-Meldung folgen, die angibt, dass das Gerät neu gestartet wurde, um die neu geladene Konfiguration zu übernehmen. Ist dies nicht der Fall, kann beim erneuten Laden ein Fehler auftreten. Wenn SPECTRUM die Restart-Meldung nicht innerhalb von 15 Minuten nach Ausgabe der Reload-Meldung empfängt, wendet es eine Ereignisregel an, die auf dem Regeltyp „Ereignispaar“ basiert, um einen Alarm mit der Ursache „ERROR DURING ROUTER RELOAD“ auszulösen. Das folgende Diagramm stellt die Ereignisse und die Zeitplanung dar.



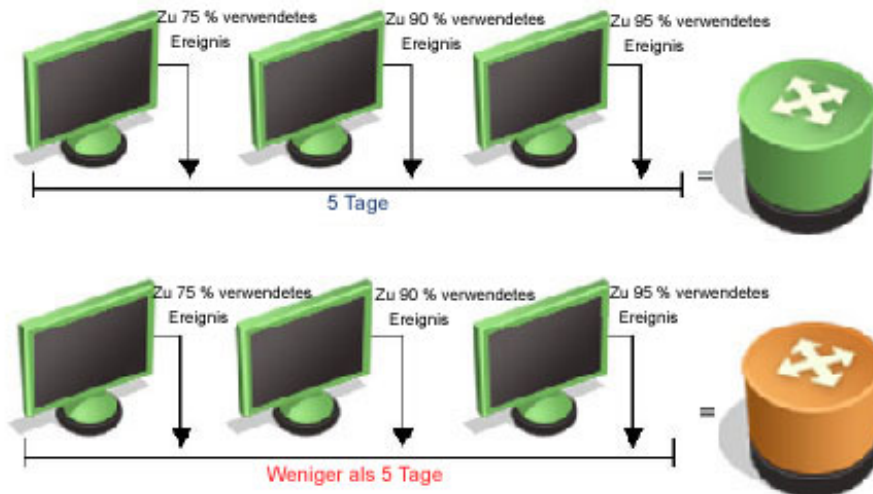
VERWALTEN VON SICHERHEITSEREIGNISSEN MIT EINER EREIGNISRATENZÄHLER-REGEL

SPECTRUM kann Ereigniszuführungen aus vielen Quellen aufnehmen. Manche Kunden senden Ereignisse von Sicherheitsgeräten aus, wie Intrusion Detection Systems (IDSs) und Firewalls. Diese Arten von Geräten können Millionen von Protokolldateieinträgen generieren. Solche Kunden können mit Hilfe einer Ereignisratenzähler-Regel zwischen sporadischen Client-Verbindungsablehnungen und echten Sicherheitsangriffen unterscheiden. Die Regel generiert einen kritischen Alarm, wenn 20 oder mehr Verbindungsfehler innerhalb von einer Minute auftreten, wie in der folgenden Abbildung dargestellt.



VERWALTEN DES SERVERSPEICHERZUWACHSES MIT HILFE EINER EREIGNISABFOLGEREGEL

Ein häufiges Problem bei einigen Anwendungen ist die Unfähigkeit, die Speicherauslastung zu verwalten. Durch manche Anwendungen wird der Systemspeicher belegt und nie wieder zur Verwendung durch andere Anwendungen freigegeben. Dadurch kann die Performance des Hostcomputers herabgesetzt werden, wodurch früher oder später die Anwendung mit dem Speicherleck abstürzt. Wenn in Ihrem System beispielsweise eine Webserveranwendung vorhanden ist, bei der bereits Probleme mit Speicherlecks aufgetreten sind, könnten Sie beispielsweise in einem geplanten Wartungsfenster einen wöchentlichen Neustart einplanen, um den Speicherverbrauch auszugleichen. Wenn das Speicherleck jedoch größer als sonst ist, also eine Abweichung vom Normalverhalten eintritt, sollten Sie eventuell einen Notneustart vor der eingeplanten Wartung ausführen. Sie können mit Hilfe einer Kombination aus progressiven SPECTRUM-Schwellenwerten mit einer Ereignisabfolgeregel das System auf abnormes Verhalten überwachen oder über die eHealth Live Health-Analyse einen Bericht über die Abweichung vom normalen Speicherverbrauch erstellen. Mit den SPECTRUM-Schwellenwerten als Beispiel würde das bedeuten, dass die Überwachung Ereignisse generiert, wenn die Speicherbelegung die Schwellenwerte von 50 %, 75 % und 90 % übersteigt. Wenn diese Schwellenwerte in weniger als einer Woche erreicht werden, generiert SPECTRUM einen Alarm, um die Benachrichtigung zum Neustart des Servers vor Beginn des eingeplanten Wartungsfensters auszugeben. Dies ist im folgenden Diagramm dargestellt.



KOMBINATION EINER VORDEFINIERTEN EREIGNISBEDINGUNGSREGEL MIT EINER EREIGNISPAARREGEL

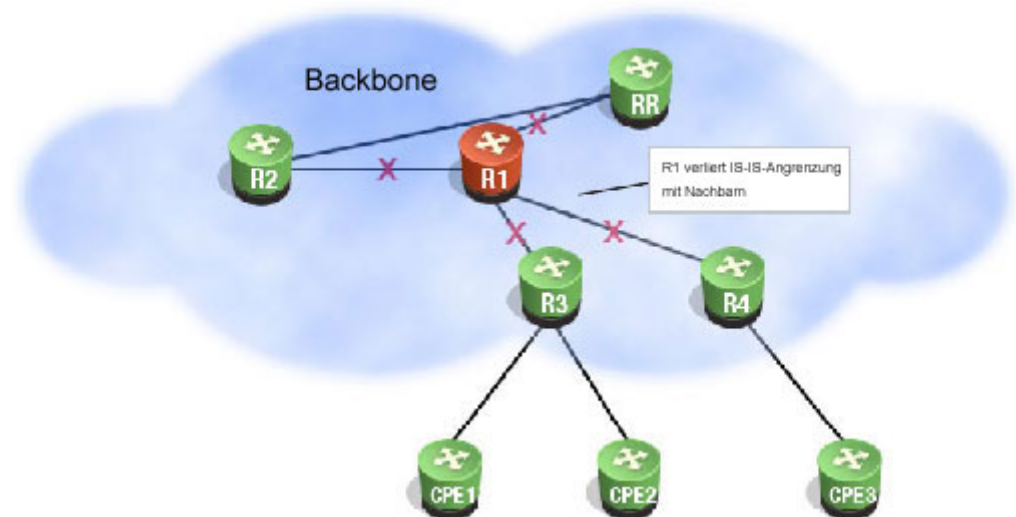
RFC2668 (MIB für IEEE 802.3 Medium Attachment Units) enthält Managementdefinitionen für Ethernet-Hubs. Im RFC wird über die Definition eines SNMP-Traps ein Management-System benachrichtigt, wenn sich der Jabber-Status eines Interfaces ändert. Jabber tritt auf, wenn ein Gerät mit elektronischen Störungen oder logischen Fehlern fortlaufend Ausschussdaten sendet. Der Trap-Bezeichner zeigt einfach eine Änderung des Zustands an und der variable Datenteil des Traps gibt an, ob das „Jabbern“ begonnen oder aufgehört hat. SPECTRUM wendet eine Ereignisbedingungsregel an, um unterschiedliche Start-/Stoppereignisse anhand des variablen Teils des Traps zu generieren, und setzt eine Ereignispaarregel ein, um einen Alarm zu erzeugen, wenn das „Jabberstart“-Ereignis nicht von einem „Jabberstopp“-Ereignis gefolgt wird.

TECHNOLOGIE ZUR KORRELATION VON BEDINGUNGEN

Die CA SPECTRUM CCT bietet erweiterte Anpassungsfunktionen zum Definieren von Ereignisbeziehungen, durch die die Ursachen von Problemen isoliert werden können. Betrachten Sie beispielsweise die Komplexität der Verwaltung eines IP-Netzwerks, das VPN-Konnektivität für einen MPLS-Backbone mit bereichsinternem, über Intermediate System-to-Intermediate System (IS-IS) verwaltetem Routing und bereichsübergreifendem, über BGP verwaltetem Routing bietet. Jegliche Fehler an physischen Verbindungen oder Protokollen könnten Dutzende von Ereignissen von mehreren verschiedenen Geräten auslösen. Ohne die Anwendung hoch entwickelter Korrelationsverfahren würden die mit der Netzwerkproblemlösung betrauten Techniker viel Zeit damit vergeuden, Symptome zu verfolgen, anstatt die Ursache zu beheben.

BEISPIEL: IS-IS-ROUTING-FEHLER

Das folgende Beispiel veranschaulicht die Anwendungsmöglichkeiten der Korrelation von Bedingungen. Ein Kernrouter, in der Abbildung als R1 bezeichnet, hat die IS-IS-Nachbarschaft zu allen Nachbarn (in der Abbildung R2, R3 und R4) verloren. Dadurch wird auch die BGP-Sitzung mit dem Route Reflector (in der Abbildung als RR bezeichnet) gestört. Wenn diese Bedingung bestehen bleibt, veraltet das von R1 und den benachbarten Edge Routern R3 und R4 ausgehende Routing. Über kurz oder lang werden die VPN-Sites des Kunden, die von diesen Edge Routern versorgt werden, ihre Peer-Sites (in der Abbildung bezeichnet als CPE1, CPE2, CPE3) nicht mehr erreichen können.



Durch diesen Fehler generieren die Router eine Reihe von Syslog-Fehlermeldungen und Traps. Die folgende Tabelle enthält die Meldungen und Traps, die SPECTRUM empfangen würde:

Source	Type	Message
R1	Syslog message	%CLNS-5-ADJCHANGE: ISIS: Adjacency to R2 (POS5/0/0) Down, hold time expired
R1	Syslog message	%CLNS-5-ADJCHANGE: ISIS: Adjacency to R3 (POS5/0/0) Down, hold time expired
R1	Syslog message	%CLNS-5-ADJCHANGE: ISIS: Adjacency to Rn (POS5/0/0) Down, hold time expired
R1	Syslog message	%BGP-5-ADJCHANGE: neighbor R1 Down BGP Notification sent
R1	Syslog message	%BGP-3-NOTIFICATION: sent to neighbor R1 4/0 (hold time expired) 0 bytes
R1	Trap	BGP Backwards Transition trap, neighbor = R1
R2	Syslog message	%CLNS-5-ADJCHANGE: ISIS: Adjacency to R1 (POS5/0/0) Down, hold time expired
R3	Syslog message	%CLNS-5-ADJCHANGE: ISIS: Adjacency to R1 (POS5/0/0) Down, hold time expired
Rn	Syslog message	%CLNS-5-ADJCHANGE: ISIS: Adjacency to R1 (POS5/0/0) Down, hold time expired

Die Ursache all dieser Meldungen ist der Fehler des IS-IS-Routings in Zusammenhang mit R1. In vielen Management-Systemen würde der Bediener bzw. derjenige, der sich um die Problembehebung kümmert, diese einzelnen Meldungen und Traps als scheinbar unzusammenhängende Ereignisse auf der Ereignis-/Alarmkonsole sehen. Ein ausgebildeter Bediener oder ein erfahrener Problemlöser würde eventuell nach einigen Überlegungen folgern, dass ein Routing-Fehler an R1 besteht. In großen Umgebungen ist es jedoch wahrscheinlich, dass diese Ereignisse/Alarmer zwischen anderen Ereignissen/Alarmen auf der Konsole untergehen. Selbst wenn der Bediener oder Problemlöser ausreichend Erfahrung hätte und die Korrelation manuell identifizieren könnte, wäre dazu viel Zeit und Aufwand erforderlich. Diese Zeit hängt direkt mit Kosten, geringerer Benutzerzufriedenheit und verlorenen Einnahmen zusammen.

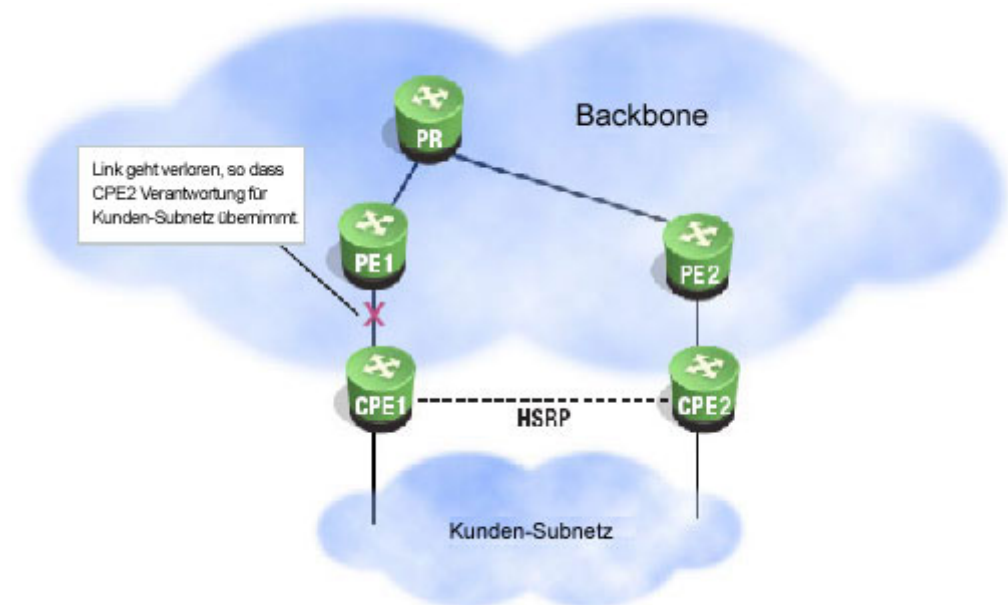
Ohne die Korrelation von Bedingungen würde SPECTRUM dem Benutzer auf der Alarmkonsole Benachrichtigungen über zehn oder mehr Ereignisse anzeigen. Mit einer Kombination aus einer Ereignisregel und der Korrelation von Bedingungen können Sie ein Set von Regelmustern auf eine Korrelationsdomäne, die alle Kernrouter (LSR) umfasst, anwenden, woraufhin SPECTRUM nur einen einzelnen aktionsfähigen Alarm ausgibt. Dieser Alarm zeigt an, dass für R1 ein IS-IS-Routingfehler besteht und dass es zu einem Netzausfall kommen kann, wenn dieser Fehler nicht behoben wird. Die scheinbar nicht zusammenhängenden Bedingungen, die SPECTRUM korreliert und die diesen Alarm auslösen, werden auf die folgende Weise im Fenster „Symptoms“ der Alarmkonsole angezeigt:

1. Über eine lokale Ereignisratenzähler-Regel wurden die verschiedenen Syslog-Meldungen über die Änderung der IS-IS-Nachbarschaft definiert, die von der gleichen Quelle wie ein Routingfehler für diese Quelle berichtet wurden.
2. Es wurde ein Regelmuster eingesetzt, um ein Ereignis über den Verlust der IS-IS-Nachbarschaft zu generieren, das durch einen IS-IS-Routingfehler „verursacht“ wurde, wenn der Nachbar des Ereignisses der verlorenen Nachbarschaft mit der Quelle des Routingfehler-Ereignisses übereinstimmt.

3. Es wurde ein Regelmuster eingesetzt, um ein Ereignis über den Ausfall der BGP-Nachbarschaft zu generieren, das durch einen IS-IS-Routingfehler „verursacht“ wurde, wenn der Nachbar des Ereignisses der ausgefallenen Nachbarschaft mit der Quelle des Routingfehler-Ereignisses übereinstimmt.
4. Es wurde ein Regelmuster eingesetzt, um ein Ereignis über den BGP-Rückübergangs-Trap zu generieren, das durch einen IS-IS-Routingfehler „verursacht“ wurde, wenn der Nachbar des Rückübergangs-Ereignisses mit der Quelle des Routingfehler-Ereignisses übereinstimmt.

BEISPIEL: HSRP/VRRP-ROUTINGFEHLER

Durch die Korrelation von Bedingungen kann auch eine interessante und hilfreiche Korrelation von Ereignissen entstehen, wenn eine Verbindung zu einem Router in einer Hot Standby Routing Protocol (HSRP)- oder Virtual Router Redundancy Protocol (VRRP)-Umgebung unterbrochen wird. Im folgenden Beispiel verfügt ein Standort über zwei redundante Router, die Zugriff über HSRP ermöglichen. In diesem Fall liegt am primären Router ein Fehler vor, der redundante Router jedoch versorgt weiterhin den Kundenstandort. Sie möchten eventuell über den Ausfall des redundanten Routers eine Alarmbenachrichtigung erhalten, in der zu einem vollständigen Standortausfall unterschieden wird. Kenntnisse über IMT, EMS und CCT können bei der RCA hilfreich sein.



In der folgenden Tabelle werden die Syslog-Fehlermeldungen und Trap-Abfolgen für den HSRP-Ausfall dargestellt.

Quelle	Typ	Meldung
PE1	Syslog-Meldung	%LINK-3-UPDOWN: Interface Serial0/1 changed start to down
PE1	Trap	Link down trap, ifIndex=5, ifOperStatus=Down
PE2	Trap	HSRPGrpStandByState, state=Active
NMS	Fehlgeschlagene Abfrage	Device Contact Status Lost, Model=CPE1

Die scheinbar unzusammenhängenden Bedingungen, die SPECTRUM korreliert hat, um diesen Alarm zu melden, werden im Fenster „Symptoms“ der Alarmkonsole folgendermaßen angezeigt:

1. Eine Korrelationsdomäne, die nur aus den zwei CPE-HSRP-Routern besteht, und die PE-Router-Interfaces, über die diese Standorte verbunden werden.
2. Ein Regelmuster, das das Zusammentreffen eines HSRPGrpStandByState-Ereignisses mit einem aktiven Status und ein Gerätekontaktverlust-Ereignis korreliert, um eine Primärverbindungsverlust-Bedingung abzuleiten.
3. Ein Regelmuster, das ein Ereignis einer fehlerhaften Verbindung definiert, das durch ein Primärverbindungsverlust-Ereignis verursacht wurde.

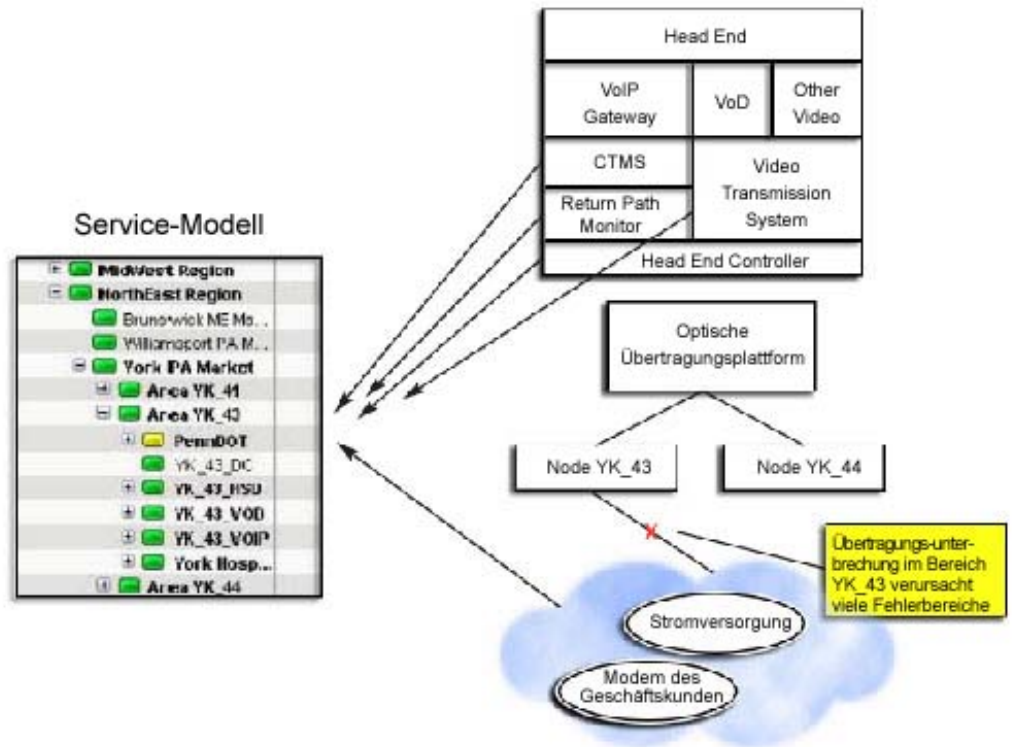
Diese Regelmuster werden auf die HSRP-Korrelationsdomänen angewendet, um jegliche Korrelationen außerhalb dieses Bereichs zu verhindern.

Ohne diese Regeln hätte SPECTRUM einen kritischen Alarm für das getrennte CPE-Gerät und das verbundene Portmodell ausgelöst. Durch diese Regeln wird ein schwerwiegender Alarm (orange) für das CPE-Gerät ausgelöst, der angibt, dass die Primärverbindung zum Kunden unterbrochen ist. Die anderen Bedingungen werden in der Symptomtabelle für diesen Alarm angezeigt.

Anwendung der Bedingungskorrelation auf die Korrelation von Services

Normalerweise beinhalten und unterstützen Netzwerke mehr als einen Service. In der Kabelindustrie beispielsweise werden Telefonservice (VoIP), Internetzugriff (High Speed Data), VoD und Digitalkabel über das gleiche physische Datennetzwerk bereitgestellt. Das Verwalten dieses Netzwerks kann eine echte Herausforderung darstellen. Im Netzwerk (Kabelanlage) arbeiten die Videoübertragungseinrichtungen, die Videoabonnementservices und das Cable Model Termination System (CMTS) zusammen, um Daten in das Kabelnetzwerk mit den richtigen Frequenzen zu übertragen. Unzählige Kilometer von Kabel und Tausende von Verstärkern und Stromversorgungseinrichtungen müssen die Signale in die Heime von Millionen von Abonnenten übertragen.

Wenn die Netzwerkleitungen wie im folgenden Diagramm dargestellt an einer Stelle unterbrochen sind, melden das Rückleitungsüberwachungssystem und der Head-End-Controller Probleme bei der Rückleitung oder der Stromversorgung in diesem Bereich. Das CMTS würde die Anzahl der Kabelmodems für den Knoten angeben, die offline sind. Das Videoübertragungssystem würde Abstimmungsfehler für Videoabonnements in diesem Bereich generieren. Zuletzt würde das Management-System den Kontakt mit jeglichen Geschäftskundenmodems, die es verwaltet, verlieren. Bei der Flut an Ereignissen und Fehlermeldungen für die verwalteten Elemente ist es offensichtlich, dass für den Service Fehler vorliegen. Die Herausforderung besteht darin, aus diesen Daten die Ursache und die für die Auswirkungen auf den Service relevanten Informationen herauszufiltern.



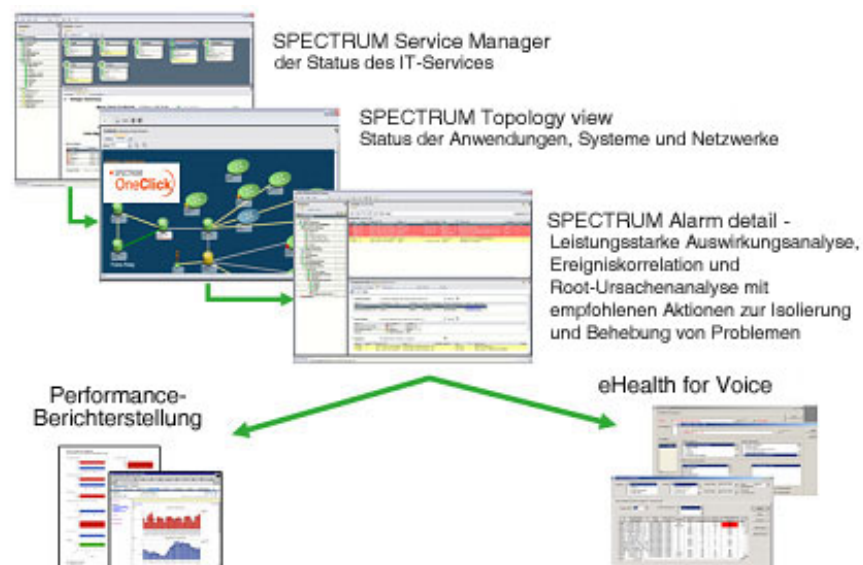
SPECTRUM kann die Fülle an Ereignissen interpretieren, indem es den Servicebereich der scheinbar zusammenhanglosen Ereignisse als einen Faktor in die Korrelation der Bedingungen einbezieht. Durch das Modellieren der Servicebereiche und Services in SPECTRUM kann mit Hilfe der Korrelation der Bedingungen bestimmt werden, welche Services in welchen Bereichen betroffen sind, und es kann/können die Ursache(n) identifiziert werden.

Die Relevanz der Serviceauswirkungen geht über die Kenntnisse dazu hinaus, welche Elemente betroffen sind, denn es ist ebenso wichtig, zu bestimmen, auf welche Elemente *keine* Auswirkungen bestehen. Es ist möglich, dass der Videoabonnementservice an einen einzelnen Servicebereich keine VoD-Inhalte liefert, und doch alle anderen Services für diesen Bereich normal funktionieren. In einem anderen Fall könnte ein Rückleitungsfehler in einem Bereich Fehlfunktionen der Internet-, VoIP- und VOD-Services sowie eine Beeinträchtigung der Leistung des Digitalkabels bewirken, wohingegen die Funktion des Analogkabels nicht beeinträchtigt wäre. Mit den Funktionen von SPECTRUM und den Ansichten Ihrer Infrastruktur können Sie die Ursache schneller und einfacher erkennen und sich zuerst auf die Lösung des Problems konzentrieren.

Effektiver Einsatz der integrierten Lösung

Nachdem SPECTRUM die Ursachenprobleme identifiziert hat, kann das Bedienpersonal auf schnelle Weise durch Navigieren von den Alarmen im OneClick-Browser zu den eHealth- und eHealth for Voice-Berichten und -Tools Details zum Problemverlauf und Informationen zur Problemlösung sammeln. Bediener können beispielsweise in OneClick mit der rechten Maustaste auf einen Alarm klicken und eine beliebige der folgenden Aktionen ausführen:

- Zu Trend-Berichten über die Problemvariablen navigieren
- Zu Übersichtsberichten navigieren, um zu einer Momentaufnahme verschiedener Schlüsselperformancevariablen für diese Ressource zu gelangen
- Zur eHealth for Voice-Konsole oder eHealth-Web-Reporting-Schnittstelle navigieren, um weitere Berichte und Details zu den fehlerhaften Voice-PBX-Systemen und Anrufmeldungsservern einzusehen
- Einen Browser zur eHealth-Web-Reporting-Schnittstelle starten, um weitere Berichte und Details zu Problemressourcen anzuzeigen



(Diese Seite wurde absichtlich leer gelassen)

Index

A

- Agenten von Drittherstellern, 81
- Agenten, unterstützt, 82
- Alarm Notification Manager, 46
- Alarmdetailbericht, 153
- Alarmer bei Normabweichungen, 35
- Alarmer bei zeitlicher Überschreitung von Schwellenwerten, 35
- Alarmregeln, 71
- Alarmunterdrückung, 191
- Antwortzeittests, 118
- Assurance Server Infinity, 44
- Assurance Server Xsight, 43
- Assurance Server-Komponenten, 43
- ATM Circuit Manager, 47
- Ausfallzeiten, Kosten, 14
- Ausnahmebereich, Senden von Traps, 152
- Ausnahmenzusammenfassungsbericht, 162

B

- Bedingungen, SPECTRUM, 184
- Bericht zu unterbeanspruchten Elementen, 156
- Best Practices, 157
- Berichte
 - Health, 74, 92
 - Konditionale Kapazitätstrend-Berichte, 96
 - MyHealth-Berichte, 92
 - Top-N-Berichte, 96
 - Trend-Berichte, 94
 - Übersichtsberichte, 91
- Business Objects, Installation, 62
- Business Service Intelligence (BSI), 97
- Business Service Management (BSM), 97

C

- CA Green Book, Ziel, 9
- CA Technology Services, 13
 - Angebote, 30
- Capacity Analyzer, 173
 - Best Practices, 175
- CA-Reifemodelle, 32
- Cisco-Syslog-Meldungen, 192
- Cluster, eHealth, 41
- Community-Zeichenfolge, 81
- Configuration Manager, 50

D

- Das Ereignis-Management-System, 182
- Database Manager, eHealth for Voice, 63

- Detailbericht für zu beobachtende Situationen, 167
- Diagramm für zu beobachtende Situationen, 167
- Distributed eHealth, 41

E

- E2E Console, 39
- eHealth
 - Komponenten, 26
 - Report Developer Language (RDL), 42
 - sichern, 79
 - Sizing Wizard, 57
 - SPECTRUM-Integration, 28
 - Vorteile, 26
 - Weiterleitung von Live Health-Traps, 73
 - Zertifizierungsseiten, 40
- eHealth for Voice, 29
 - Komponenten, 53
 - Nutzungsrechtlizenz, 54
 - Policy Manager, 54
 - Senden von Traps, 152
 - sichern, 79
 - Weiterleitung von Traps an SPECTRUM, 76
- for Voice
 - Policy Manager, 150
 - geplante Discovery, 69
- Einstellungen im Dialogfeld "Create Model by IP Address", 88
- Enterprise IT Management (EITM), 12
- Enterprise Management, 20
- Entwicklung von Netzwerken, 14
- Ereignisregeltypen, 183
- Erlang, 175
- Event-to-Resolution Readiness Assessment, 13

F

- Fehlerszenarien, 115
- Frame Relay Manager, 46

G

- Gewährleistungen
 - SLA, 120
- Global Selections, 65
- Grade of Service (GoS), 174

- Gruppen
 - einer Gruppenliste hinzufügen, 69
 - erstellen, 68
 - Verwendungszweck, 68
- Gruppenlisten, Verwendungszweck, 68

H

- Health-Berichte, 74
 - Systeme, 92
 - Weiterleitung von Traps, 74
- Heterogene Netzwerke, 11

I

- Implementation
 - groß, 55
 - kleine und mittelständische Unternehmen, 55
 - Typen, 54
- Implementationsbeispiel, 60
- Installation
 - Voraussetzungen, 60
- Installationsschritte, 61
- InstallPlus-Kit, 62
- Integration
 - SPECTRUM, 28
 - Integrationsmodule (IMs), 40
 - Wert, 12
- Integrierte Lösung, Konfiguration, 64
- IT-Ressourcen, 20

K

- Kapazitätsänderungen, planen, 166
- Kapazitätsbereitstellungsberichte, 168
- Kapazitätsplanung, 155
 - Änderungen, 172
 - Sprache
 - Best Practices, 175
 - Nachrichtenspeicherkapazität, 177
 - ROI, 176
 - Services, 173
 - überbeanspruchte Ressourcen, 176
 - unterbeanspruchte Ressourcen, 176
- Kapazitätsplanung
 - Sprache
 - Erlangs, 175
 - Grade of Service, 174
 - Verbindungen, 175
 - Trends beobachten, 167
 - Trends vorhersagen, 168
 - Vorlaufzeit, 170
- Kapazitätsprojektionsberichte, 168
- Knotenlizenzen, 54
- Konditionale Berichte, 96
- Konditionale Berichte
 - ausführen, 171
- Konditionaler Kapazitätstrendbericht, 165
- Konditionaler Kapazitätstrendbericht
 - ausführen, 171

- Konfiguration
 - aktualisieren, 161
 - Best Practices, 65
 - Schritte, 64
- Konvergente Netzwerke, 15
 - Herausforderungen, 16
- Korrelationsdomänen, 185
- Korrelationsrichtlinien, 186
- Kundennahe Berichte, 132

L

- Lebenszyklus von Best Practices, 30
- Live Exceptions
 - Profile, 72
 - Servicealarmfälle, 151
 - starten, 72
- Live Health, 40
 - Profile, 71
 - Weiterleitung von Traps an SPECTRUM, 73
- Live Trend, 92

M

- Matrixtabelle für den Servicezustand, 105
- Modeling Gateway, 188
- Modelle, SPECTRUM, 181
- Multicast Manager, 48
- MyHealth-Berichte, 92

N

- Nachbarn, 189
- Netzwerk- und Sprachmanagement-Lösung, 12
- Netzwerk- und Sprachmanagement-Strategie, 21
- Netzwerkfehler und
 - Leistungsprobleme, 11
- Netzwerkfehler-Management,
 - Komponenten, 43
- Netzwerkleistungs-Management,
 - Komponenten, 39
- Netzwerkmanagement-Lösungen, 11
- Netzwerkunterstützung, 11

O

- OneClick
 - Löschen von Alarmen, 152
 - SPECTRUM, 44
- OneClick for -Konsole, 68
- Operational Support System (OSS), 23

P

- Proaktive
 - Servicesicherung, 35, 150
- Prozessregeln, 113

Q

QoS Manager, 48

R

Regeln bei Normabweichungen, 151
Regeln bei zeitlicher Überschreitung von Schwellenwerten, 151
Regierungen, 24
Remote Poller, 41
Report Center, 42
Report Manager
 SPECTRUM, 51
 Zugriff, 132
Ressourcenüberwachung, 103
Return on Investment (ROI), 160
RFC 2790
 Erweiterungen, 82
 Unterstützung für
 Prozessmodellierung, 114
RMON2-Probes, 42
Rollenbasierte Serviceinformationen, 11

S

Schnelle Lösung von Problemen, 36, 178
Secure Domain Manager (SDM), 50
Service Desk-Tickets, 153
Service Editor, 114
Service Management-Modul, 97
Service Manager, 52
Service Performance Manager (SPM), 52
Serviceanbieter, 23
Serviceanbieter im Bereich
 Telekommunikation, 23
Servicebereitstellungsplattform, 14
Service-Dashboard, 53
Servicehierarchien, 103
Service-Level-Management, 34
Servicemanagement
 Ansatz, 97
 Interviewprozess, 98
 Zuordnungsverfahren, 99
Servicemodellierung, 103
 Antwortzeit, 117
 Entwurf von Richtlinien, 106
 erstellen, 104
 Fehlerszenarien, 115
 Prozessregel, 113
 Tabelle für Servicezustand, 105
Servicesicherung, 150
Serviceumfang der eHealth-Prüfung, 33
Serviceverfügbarkeit, 19
 Berichte, 132
Servicezustand, 103
Sicherungen, archivieren, 79
Sizing Wizard, 57
Skalierung, 11

SLA

Berichte, 132
Geschäftszeiten, 121
Gewährleistungen, 120
Implementierung, 129
Komponenten, 129
Überwachung, 121
Zeiträume, 120
SLA-Modellierungskonzepte, 120
SNMPv3-Unterstützung, 49
Software- und
 Hardwareanforderungen, 57, 58
 OneClick, 58
 SPECTRUM, 58
 Voice, 59
Solution Architecture Overview (SAO), 31
Solution Architecture
 Specification (SAS), 32
SpectroSERVER, 61
SPECTRUM
 Anzeigen von Alarmen, 78
 Discovery, 65
 eHealth-Integration, 28
 Komponenten, 27
 Konfiguration von , 77
 OneClick, 44
 Service Manager, 34
 sichern, 79
 Vorteile, 28
 Watch Editor, 45
SPECTRUM Alarm Notification Manager (SANM), 46
SPECTRUM Integrity, 44
SPECTRUM Report Manager, 51
Speicherkapazität für
 Sprachnachrichten, 177
Speicherkapazität,
 Nachrichtenserver, 177
Sprache, Kapazitätsplanung, 173
Sprachservices, Netzwerk, 29
Syslog-Meldungen, 192
Systemagenten, Best Practices zur
 Überwachung, 81
SystemEDGE-Agenten, 81
Systemüberwachung, 81
Systemvoraussetzungen, 61

T

Technologie zur Korrelation von
 Bedingungen (CCT), 195
Top-N-Berichte, 96
Topologie, 87, 188
Traffic Accountant, 42
Traps
 Weiterleitung aus an SPECTRUM, 73
 Weiterleitung aus
 Health-Berichten, 74
 Weiterleitung aus Voice, 76
Trend-Berichte, 94

U

- Überlastete Ressourcen
 - Änderungen modellieren, 165
 - beseitigen, 165
 - bestätigen, 163
 - den Verlauf der Hinweise
 - dokumentieren, 165
 - feststellen, 162
- Übersichtsberichte, 91
- Überwachungen, SPECTRUM, 45
- Unicenter NSM-Agenten, 81
 - erkennen in SPECTRUM, 89
- Unterbeanspruchte Ressourcen
 - bestätigen, 158
 - Problem lösen, 159
 - Return on Investment, 160
 - suchen, 156
- Unternehmen, 24
- Ursache, 103

V

- Verfahren zur induktiven Modellierung (IMT), 181
- Vorausschauende
 - Kapazitätsplanung, 37, 155
- Vorteile, 26
 - for Voice, 29
 - SPECTRUM, 28
- VPN Manager, 49

W

- Watch Editor, 45

Z

- Zielgruppe, 9
- Zivil- und Verteidigungsbehörden, 24